Benutzerhandbuch
Revision 1.0

McAfee® GroupShield™

Version 7.0

Für Microsoft® Exchange

McAfee®

COPYRIGHT

Copyright © 2007 McAfee, Inc. Alle Rechte vorbehalten.

Diese Veröffentlichung darf in keiner Form und in keiner Weise ohne die schriftliche Genehmigung von McAfee, Inc., oder ihren Lieferanten und angeschlossenen Unternehmen ganz oder teilweise reproduziert, übertragen, in einem Abrufsystem gespeichert oder in eine andere Sprache übersetzt werden.

MARKEN

ACTIVE FIREWALL, ACTIVE SECURITY, ACTIVESECURITY (AND IN KATAKANA), ACTIVESHIELD, CLEAN-UP, DESIGN (STYLIZED E), DESIGN (STYLIZED N), ENTERCEPT, EPOLICY ORCHESTRATOR, FIRST AID, FOUNDSTONE, GROUPSHIELD, GROUPSHIELD (AND IN KATAKANA), INTRUSHIELD, INTRUSION PREVENTION THROUGH INNOVATION, MCAFEE, MCAFEE (AND IN KATAKANA), MCAFEE AND DESIGN, MCAFEE.COM, MCAFEE VIRUSSCAN, NET TOOLS, NET TOOLS (AND IN KATAKANA), NETSCAN, NETSHIELD, NUTS & BOLTS, OIL CHANGE, PRIMESUPPORT, SPAMKILLER, THREATSCAN, TOTAL VIRUS DEFENSE, VIREX, VIRUS FORUM, VIRUSCAN, VIRUSSCAN, VIRUSSCAN (AND IN KATAKANA), WEBSCAN, WEBSHIELD, WEBSHIELD (AND IN KATAKANA) sind eingetragene Marken oder Marken von McAfee, Inc. und der angeschlossenen Tochterunternehmen in den USA und anderen Ländern. Die Farbe Rot in Kombination mit „Sicherheit" ist ein Merkmal der McAfee-Markenprodukte. Alle anderen eingetragenen und nicht eingetragenen Marken in diesem Dokument sind das alleinige Eigentum der jeweiligen Inhaber.

INFORMATIONEN ZUR LIZENZ

Lizenzvertrag

HINWEIS FÜR ALLE BENUTZER: LESEN SIE DEN LIZENZVERTRAG FÜR DIE VON IHNEN ERWORBENE SOFTWARE SORGFÄLTIG DURCH. ER ENTHÄLT DIE ALLGEMEINEN BESTIMMUNGEN UND BEDINGUNGEN FÜR DIE VERWENDUNG DER LIZENZIERTEN SOFTWARE. WENN SIE NICHT WISSEN, WELCHEN SOFTWARE-LIZENZTYP SIE ERWORBEN HABEN, SCHLAGEN SIE IN DEN KAUFUNTERLAGEN, IN WEITEREN UNTERLAGEN ZUR LIZENZGEWÄHRUNG ODER IN DEN BESTELLUNTERLAGEN NACH, DIE SIE ZUSAMMEN MIT DEM SOFTWAREPAKET ODER SEPARAT ERHALTEN HABEN (ALS BROSCHÜRE ODER ALS DATEI AUF DER PRODUKT-CD ODER AUF DER WEBSEITE, VON DER SIE AUCH DAS SOFTWAREPAKET HERUNTERGELADEN HABEN). Wenn Sie mit den BESTIMMUNGEN DIESES LIZENZVERTRAGS nicht einverstanden sind, unterlassen Sie die Installation der Software. FALLS ZUTREFFEND, KÖNNEN SIE DAS PRODUKT UNTER RÜCKERSTATTUNG DES VOLLEN KAUFPREISES AN MCAFEE ODER AN DEN HÄNDLER, BEI DEM SIE DAS PRODUKT ERWORBEN HABEN, ZURÜCKGEBEN.

Hinweise

Dieses Produkt enthält möglicherweise:

• Software, die im Projekt „OpenSSL" zur Verwendung im OpenSSL Toolkit entwickelt wurde (http://www.openss1.org/). • Kryptografie-Software von Eric Young und Software von Tim J. Hudson. • Einige Softwareprogramme, für die der Benutzer eine Lizenz (oder Unterlizenz) unter GNU General Public License (GPL) oder anderen ähnlichen freien Softwarelizenzen hält, die es dem Benutzer unter anderem erlauben, bestimmte Programme oder deren Teile zu kopieren, zu ändern und weiter zu verbreiten, und die Zugriff auf den Quellcode gewähren. GPL erfordert, dass der Quellcode der der GPL unterliegenden Software, die in ausführbarem Binärformat an andere Personen weiterverbreitet wird, auch diesen Benutzern verfügbar gemacht wird. Für solche Software, die der GPL unterliegt, wird der Quellcode auf dieser CD zur Verfügung gestellt. Falls eine Lizenz für kostenlose Software erfordert, dass McAfee Rechte für die Nutzung, das Kopieren oder Ändern eines Softwareprogramms gewährt, die über die in diesem Vertrag gewährten Rechte hinausgehen, haben Rechte dieser Art Vorrang vor den Rechten und Einschränkungen in diesem Vertrag. • Ursprünglich von Henry Spencer geschriebene Software. Copyright 1992, 1993, 1994, 1997 Henry Spencer. • Ursprünglich von Robert Nordier geschriebene Software. Copyright © 1996-7 Robert Nordier. • Von Douglas W. Sauder geschriebene Software. • Von Apache Software Foundation entwickelte Software (http://www.apache.org). Eine Kopie der Lizenzvereinbarung für diese Software finden Sie unter www.apache.org/licenses/LICENSE-2.0.txt. • Internationale Komponenten für Unicode („ICU") Copyright © 1995-2002 International Business Machines Corporation und andere. • Software, die von CrystalClear Software, Inc., entwickelt wurde, Copyright (C) 2000 CrystalClear Software, Inc. • FEAD® Optimizer®-Technologie, Copyright Netopsystems AG, Berlin, Deutschland. • Outside In® Viewer Technology ©1992-2001 Stellent Chicago, Inc. und/oder Outside In® HTML Export, © 2001 Stellent Chicago, Inc. • Software mit Copyright bei Thai Open Source Software Center Ltd. und Clark Cooper, © 1998, 1999, 2000. • Software mit Copyright bei Expat maintainers. • Software mit Copyright bei The Regents of the University of California, © 1996, 1989, 1998-2000. • Software mit Copyright bei Gunnar Ritter. • Software mit Copyright bei Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A., © 2003. • Software mit Copyright bei Gisle Aas. © 1995-2003. • Software mit Copyright bei Michael A. Chase, © 1999-2000. • Software mit Copyright bei Neil Winton, ©1995-1996. • Software mit Copyright bei RSA Data Security, Inc., © 1990-1992. • Software mit Copyright bei Sean M. Burke, © 1999, 2000. • Software mit Copyright bei Martijn Koster, © 1995. • Software mit Copyright bei Brad Appleton, © 1996-1999. • Software mit Copyright bei Michael G. Schwern, ©2001. • Software mit Copyright bei Graham Barr, © 1998. • Software mit Copyright bei Larry Wall und Clark Cooper, © 1998-2000. • Software mit Copyright bei Frodo Looijaard, © 1997. • Software mit Copyright bei der Python Software Foundation, Copyright © 2001, 2002, 2003. Eine Kopie des Lizenzvertrags für diese Software finden Sie unter www.python.org. • Software mit Copyright bei Beman Dawes, © 1994-1999, 2002. • Software geschrieben von Andrew Lumsdaine, Lie-Quan Lee, Jeremy G. Siek © 1997-2000 University of Notre Dame. • Software mit Copyright bei Simone Bordet & Marco Cravero, © 2002. • Software mit Copyright bei Stephen Purcell, © 2001. • Von Indiana University Extreme! Lab entwickelt wurde (http://www.extreme.indiana.edu/). • Software mit Copyright bei International Business Machines Corporation und anderen, © 1995-2003. • Software entwickelt von der University of California, Berkeley und ihren Beitragenden.. • Software entwickelt von Ralf S. Engelschall <rse@engelschall.com> zur Verwendung im mod_ssl-Projekt (http:// www.modssl.org/). • Software mit Copyright bei Kevlin Henney, © 2000-2002. • Software mit Copyright bei Peter Dimov und Multi Media Ltd. © 2001, 2002. • Software mit Copyright bei David Abrahams, © 2001, 2002. Informationen zur Dokumentation finden Sie unter http://www.boost.org/libs/bind/bind.html. • Software mit Copyright bei Steve Cleary, Beman Dawes, Howard Hinnant & John Maddock, © 2000. • Software mit Copyright bei Boost.org, © 1999-2002. • Software mit Copyright bei Nicolai M. Josuttis, © 1999. • Software mit Copyright bei Jeremy Siek, © 1999-2001. • Software mit Copyright bei Daryle Walker, © 2001. • Software mit Copyright bei Chuck Allison und Jeremy Siek, © 2001, 2002. • Software mit Copyright bei Samuel Krempp, © 2001. Informationen zu Aktualisierungen, zur Dokumentation und zum Revisionsverlauf finden Sie unter http://www.boost.org. • Software mit Copyright bei Doug Gregor (gregod@cs.rpi.edu), © 2001, 2002. • Software mit Copyright bei Cadenza New Zealand Ltd., © 2000. • Software mit Copyright bei Jens Maurer, ©2000, 2001. • Software mit Copyright bei Jaakko Järvi (jaakko.jarvi@cs.utu.fi), ©1999, 2000. • Software mit Copyright bei Ronald Garcia, © 2002. • Software mit Copyright bei David Abrahams, Jeremy Siek und Daryle Walker, ©1999-2001. • Software mit Copyright bei Stephen Cleary (shammah@voyager.net), ©2000. • Software mit Copyright bei Housemarque Oy <http://www.housemarque.com>, © 2001. • Software mit Copyright bei Paul Moore, © 1999. • Software mit Copyright bei Dr. John Maddock, © 1998-2002. • Software mit Copyright bei Greg Colvin und Beman Dawes, © 1998, 1999. • Software mit Copyright bei Peter Dimov, © 2001, 2002. • Software mit Copyright bei Jeremy Siek und John R. Bandela, © 2001. • Software mit Copyright bei Joerg Walter und Mathias Koch, © 2000-2002. • Software mit Copyright bei der Carnegie Mellon University © 1989, 1991, 1992. • Software mit Copyright bei Cambridge Broadband Ltd., © 2001-2003. • Software mit Copyright bei Sparta, Inc., © 2003-2004. • Software mit Copyright bei Cisco, Inc. und Information Network Center of Beijing University of Posts and Telecommunications, © 2004. • Software mit Copyright bei Simon Josefsson, © 2003. • Software mit Copyright bei Thomas Jacob, © 2003-2004. • Software mit Copyright bei Advanced Software Engineering Limited, © 2004. • Software mit Copyright bei Todd C. Miller, © 1998. • Software mit Copyright bei The Regents of the University of California, © 1990, 1993, mit aus Software abgeleitetem Code, die Berkeley von Chris Torek zur Verfügung gestellt wurde.

Inhalt

1 Einführung 7

Info zu GroupShield für Exchange 7
Was ist GroupShield? 8
Wie funktioniert GroupShield? 8
Wie wird Exchange durch GroupShield geschützt? 8
Wie funktioniert ein Scan? 9
Weitere zu schützende Bereiche 10
GroupShield-Funktionen 11
Was ist neu? 12
Nicht unterstützte Funktionen 16
Verwenden dieses Handbuchs 16
Zielgruppe 17
Konventionen 17
Abrufen von Produktinformationen 18
Standarddokumentation 18
Kontaktinformationen 19

2 Vor dem Installieren 21

Szenarien vor der Installation 21
Installationsarten 22
Systemanforderungen 23

3 Installieren der Software 25

Zugreifen auf die Software 25
In der Software enthaltene Komponenten 26
Installieren von GroupShield für Microsoft® Exchange Server 2003/2007 26
Installieren von zusätzlichen Komponenten 30
Schutz vor Pufferüberläufen 31
Installieren von McAfee Anti-Spam für GroupShield 32
Hintergrundinstallation 32
Konfigurieren von GroupShield in einer Clusterumgebung 34
Aktualisieren von GroupShield von v6.0.2 oder höher 38

4 Post-Installation und Wartung 41

Testen der GroupShield-Installation 41
Testen der Virenschutzkomponente 41
Testen der Anti-Spam-Komponente 42
Testen der GroupShield-Installation mittels McAfee Virtual Technician 43
Isolieren mithilfe von McAfee Quarantine Manager 4.1 43
Aktualisieren von schwarzen und weiße Listen 44
Warten der GroupShield-Anwendung 46
Ändern der GroupShield-Installation 46
Reparieren der GroupShield-Installation 47
Wiederherstellen der Standardkonfiguration 47
Deinstallieren von GroupShield für Exchange 48

5 Integrieren in ePolicy Orchestrator 3.6 49

Einführung 49
Voraussetzungen für die Verwendung von ePolicy Orchestrator 3.6 50
Einführung in die ePolicy Orchestrator-Konsole 50
Bevor Sie beginnen 51
Installation 52
Aktualisieren von GroupShield für Exchange Version 6.0.x-NAP-Einstellungen . . . 56
Konfigurieren von GroupShield-Richtlinien 57
Verwalten von Richtlinien 57
Planen von Tasks 59
Berichte 63
Konfigurieren von Berichten 64
Deinstallation 65

6 Integrieren in ePolicy Orchestrator 4.0 67

Einführung 67
Voraussetzungen für die Installation von ePolicy Orchestrator 67
Bevor Sie beginnen 68
ePolicy Orchestrator-Agent 68
Installation 70
Einchecken des McAfee GroupShield für Microsoft Exchange Server 2003/2007-Pakets in den ePolicy Orchestrator-Server 70
Installieren von GroupShield für Exchange auf dem Clientcomputer 70
Erweiterungen 71
Einführung von ePolicy Orchestrator 4.0 Dashboard 72
Berichterstellung 74
Systeme 76
Richtlinien 77
Client-Tasks 78
Deinstallation 81

7 Integrieren in ProtectionPilot 1.5 83

Einführung . . . 83
Voraussetzungen für die Verwendung von ProtectionPilot . . . 83
Einführung in ProtectionPilot . . . 84
Bevor Sie beginnen . . . 85
Installation . . . 85
Konfigurieren von GroupShield-Richtlinien . . . 86
Einrichten und Durchsetzen von Richtlinien . . . 87
Planen von Tasks . . . 90
Erstellen eines neuen Tasks zum Scannen auf Anforderung . . . 91
Erstellen eines neuen AutoUpdate-Tasks . . . 92
Deinstallation . . . 93

8 Erste Schritte in der Benutzeroberfläche 95

Dashboard . . . 96
Statistik & Informationen . . . 97
Scans auf Anforderung . . . 99
Statusbericht . . . 103
Graphische Berichte . . . 105

9 Erkannte Elemente 107

Spam . . . 108
Phishing . . . 109
Viren . . . 110
Potenziell unerwünschte Programme . . . 111
Unerwünschter Inhalt . . . 112
Gesperrte Dateitypen/Nachrichten . . . 113
Alle Elemente . . . 113

10 Richtlinien-Manager 117

Ansichten im Richtlinien-Manager . . . 117
Vererbungsansicht . . . 118
Erweiterte Ansicht . . . 118
Erstellen einer Unterrichtlinie . . . 119
Richtlinieneinstellungen . . . 120
Alle Scanner auflisten . . . 120
Einstellungen anzeigen . . . 123
Benutzer angeben . . . 123
Scanner und Filter . . . 124
Kernscanner . . . 125
Filter . . . 148
Verschiedenes . . . 169
Gemeinsam benutzte Ressource . . . 172
Scanner und Warnungen . . . 173
Filterregeln . . . 177
Zeitintervalle . . . 180

11 Einstellungen & Diagnose 181

Einstellungen für Scan bei Zugriff 182
Benachrichtigungen 185
Anti-Spam 187
Erkannte Elemente 187
McAfee Quarantine Manager 187
Lokale Datenbank 188
Voreinstellungen für Benutzeroberfläche 189
Dashboardeinstellungen 189
Einstellungen für Grafiken und Diagramme 189
Diagnose 190
Fehlersuchprotokollierung 190
Fehlerberichterstellungsdienst 191
Ereignisprotokollierung 191
Produktprotokoll 191
Produktprotokoll 193
DAT-Einstellungen 194
Konfiguration importieren und exportieren 194

Stichwortverzeichnis 197

1 Einführung

Info zu GroupShield für Exchange

Dieses Kapitel ist eine Einführung in McAfee® GroupShield™ 7.0 und beschreibt die Funktionen zum Schutz von Microsoft® Exchange Server 2003 und Microsoft® Exchange Server 2007 gegen bösartigen und unerwünschten Inhalt.

Folgende Themen werden behandelt:

- *Was ist GroupShield?*
- *Wie funktioniert GroupShield?*
- *Wie wird Exchange durch GroupShield geschützt?*
- *An welcher Stelle im Netzwerk befindet sich GroupShield?*
- *Weitere zu schützende Bereiche*
- *GroupShield-Funktionen*
  - *Was ist neu?*
  - *Nicht unterstützte Funktionen*

Was ist GroupShield?

Die Software McAfee® GroupShield™ 7.0 schützt Microsoft® Exchange Server 2003 und Microsoft® Exchange Server 2007 vor Viren, Phishing, Spam, unerwünschtem Inhalt, potenziell unerwünschten Programmen und gesperrten Dateitypen bzw. Nachrichten. Des Weiteren wird die Inhaltsfilterung von E-Mails unterstützt.

Wie funktioniert GroupShield?

Die GroupShield-Software lässt sich in Microsoft® Exchange Server 2003/2007 integrieren und scannt E-Mails.

Jedes Mal, wenn eine E-Mail gesendet oder empfangen wird, scannt GroupShield diese und vergleicht sie mit einer Liste bekannter Viren und verdächtigem, virusähnlichem Verhalten. GroupShield kann auch auf Inhalt in der E-Mail scannen und dazu die in GroupShield definierten Regeln und Richtlinien verwenden.

Wie wird Exchange durch GroupShield geschützt?

GroupShield verwendet den McAfee®-Transport-Scanner und Microsoft® Virus Scanning API (VSAPI) zum Scannen sämtlicher E-Mails.

Bei Microsoft® Exchange Server 2003 (verwendet als Bridgeheadserver) und Microsoft® Exchange Server 2007 (mit ausschließlicher Edge-Transport- oder Hub-Transport-Funktion) verwendet GroupShield zum Schützen des Servers den McAfee®-Transport-Scanner (und nicht den Microsoft® Transport Scanner). Bei Exchange Server 2003 Mailbox Server und Exchange 2007 MailBox Role stellt GroupShield mithilfe von Microsoft VSAPI weitere Scanoptionen zur Verfügung.

Die Anti-Spam-, Antivirus- und Content-Management-Module scannen die Nachrichten und liefern das Ergebnis an GroupShield 7.0 bevor diese in das Dateisystem geschrieben und von Microsoft® Exchange 2003/2007-Benutzern gelesen werden.

Das Antivirus-Modul und das Anti-Spam-Modul vergleichen die E-Mail mit allen bekannten Signaturen der aktuell installieren Virusdefinitionsdatei (DAT) und Anti-Spam-Regeln. Das Antivirusmodul prüft außerdem die Nachricht mithilfe der ausgewählten heuristischen Erkennungsmethoden.

Das Content-Management-Modul durchsucht die E-Mail nach gesperrtem Inhalt und wendet dabei die Content-Management-Regeln der GroupShield-Software an.

Wenn in der E-Mail weder Viren noch gesperrter oder unerwünschter Inhalt entdeckt werden, übergibt GroupShield die Informationen wieder an Microsoft® Exchange 2003/2007.

Andernfalls führt GroupShield die in den Konfigurationseinstellungen definierten Aktionen durch.

Die standardmäßig durchgeführten Aktionen können unterschiedlich sein, je nachdem, welche Version von Microsoft® Exchange installiert ist und welches Scanverfahren gewählt wurde.

E-Mail-Serverschutz — McAfee GroupShield

McAfee GroupShield 7.0 fügt sich in Microsoft® Exchange Server 2003/2007 ein und bildet einen Schutz gegen Viren, die sich über Ihr unternehmenseigenes E-Mail-System verbreiten können.

Aufgrund der guten Integration von E-Mail-Server und der GroupShield-Antiviruslösung, erstreckt sich der Leistungsumfang von GroupShield über die Virenabwehr hinaus. Folgende Funktionen stehen zur Verfügung:

- Schützen des E-Mail-Servers vor schädlichen Skripts in E-Mails.
- Blockieren von Nachrichten mit bestimmten Anlagen
- Blockieren von Nachrichten mit bestimmten Wörtern in der Betreffzeile oder im Haupttext
- Blockieren von Nachrichten von bestimmten Adressen

Wie funktioniert ein Scan?

Das Kernstück der GroupShield-Software bilden das Scanmodul von McAfee® Security und die Virusdefinitionsdateien (DAT-Dateien). Das Modul führt komplexe Datenanalysen aus. Die DAT-Dateien enthalten umfangreiche Informationen, darunter Tausende verschiedene Treiber mit detaillierten Informationen zur Identifizierung eines Virus oder Virustyps.

Das McAfee® Security-Scanmodul verwendet die DAT-Dateien. Es ermittelt, welches Element gescannt wird, decodiert den Inhalt dieses Objekts und erfasst damit die Beschaffenheit des Elements. Anschließend verwendet es die Informationen in den DAT-Dateien, um nach bekannten Viren zu suchen und sie zu lokalisieren. Zahlreiche Viren haben eine eigene Signatur. Es gibt eine Folge von Zeichen, die nur einem Virus eigen ist. Das Modul sucht diese Signatur.

Das Modul verwendet außerdem bei der Suche nach unbekannten Viren eine Technik, die als heuristische Analyse bezeichnet wird. Dabei wird der Programmcode des Objekts analysiert, und es werden bestimmte Merkmale gesucht, die üblicherweise in Viren zu finden sind.

Wenn das Modul die Identität eines Virus bestätigt hat, wird versucht, das Objekt zu säubern. Dies geschieht beispielsweise durch Entfernen eines infizierten Makro aus der Anlage oder durch Löschen des Viruscode in einer ausführbaren Datei. Unter bestimmten Umständen, etwa wenn der Virus Daten zerstört hat, kann die Datei nicht repariert werden. Das Modul muss die Datei sichern, damit sie nicht aktiviert werden und andere Dateien infizieren kann.

Weitere zu schützende Bereiche

Im Rahmen einer integralen Virenschutzlösung können folgende Schlüsselbereiche Ihres Netzwerks durch McAfee® Security-Produkte geschützt werden:

- **Internet-Gateway-Schutz — Secure Content Management Appliances**

  Die größte Gefahr für Ihr Unternehmensnetzwerk bildet der Internetdatenverkehr, sei es über E-Mails oder durch die Verbindung zu Websites, die bösartigen Code enthalten. Secure Content Management Appliances schützt das Gateway zwischen Ihren internen Netzwerken und dem Internet. Der gesamte ein- und ausgehende Datenverkehr zwischen Ihrem Netzwerk und dem Internet wird gescannt. So wird verhindert, dass Viren aus dem Internet in Ihr Netzwerk gelangen.

- **Dokumentenrepository-Schutz — McAfee PortalShield**

  Die Verwendung von Computern in Unternehmensumgebungen hat die Erstellung von Dokumenten vereinfacht, die wichtige Informationen enthalten können. Mehrere Softwarehersteller bieten Portalserver an, die wichtige Dokumente für Sie speichern, indexieren und kontrollieren, sodass sie bei Bedarf leicht ausfindig gemacht werden können. Da diese Portalserver mit dem Zweck eingerichtet werden, Ihre kritischen Informationen zu speichern, hat der Schutz dieser Informationen wesentliche Bedeutung. McAfee® PortalShield™ wird in die Speicher dieser Produkte integriert. Dokumente werden jedes Mal gescannt, wenn auf sie zugegriffen wird oder wenn sie gespeichert werden.

- **Desktop- und Dateiserver-Schutz — McAfee VirusScan Enterprise**

  Nicht alle Viren werden per E-Mail übertragen. Zahlreiche Viren können sich durch Lesen von physischen Medien verbreiten, z. B. von Disketten oder CDs. Andere verbreiten sich, indem sie sich über Netzwerkfreigaben von einem Computer auf den nächsten im gesamten Netzwerk kopieren.

  Für jemanden, der Ihr Unternehmensnetzwerk angreifen möchte, bilden die Dateiserver ein gutes Ziel. An Ihre Dateiserver sind zahlreiche andere Computer angeschlossen und eine Infektion auf dem Dateiserver hat wahrscheinlich schwerwiegendere Konsequenzen als die Infektion eines Desktop-Computers.

Die McAfee® VirusScan-Serie schützt Desktop-Computer und Dateiserver in Ihrem Netzwerk. In einer integrierten Strategie gegen Viren kann VirusScan als „letzte Verteidigungslinie" beschrieben werden: Jeder Desktop-Computer und Dateiserver wird gegen Viren geschützt, die sich über Netzwerkfreigaben oder physische Medien verbreiten können.

VirusScan ist in Versionen erhältlich, die Microsoft® Windows-, Unix- und Apple Macintosh-Computer sowie die führenden drahtlosen Geräte schützen, die Sie an Ihren PC und an Ihr Netzwerk anschließen können.

- **Verwaltungslösung — McAfee® ePolicy Orchestrator**

  Mit ePolicy Orchestrator können Sie von zentraler Stelle aus alle McAfee-Antiviruslösungen im gesamten Netzwerk verwalten und aktualisieren. Damit stellen Sie sicher, dass die Module und Virusdefinitionsdateien (DAT-Dateien) aktuell sind und wirksame Richtlinien gegen Angriffe auf Ihr Netzwerk gelten.

GroupShield-Funktionen

GroupShield beinhaltet folgende Hauptfunktionen für Exchange Server 2003 und 2007:

- *Antivirusscans* — GroupShield bietet Ihnen die Möglichkeit, Virenscans an E-Mails auszuführen, die über Microsoft® Exchange SMTP übermittelt wurden, oder sich im ® Exchange Server-Speicher befinden.

- *Anti-Spam-Scans* — Spam-E-Mails werden am Arbeitsplatz zunehmend zum Problem. Spam nimmt Übertragungskapazitäten und Speicherplatz in Anspruch und verringert damit die betriebsinternen Systemressourcen; außerdem hält es die Arbeitnehmer von ihrer eigentlichen Arbeit ab, da sie sich mit den unerwünschten E-Mails in ihrem Postfach abgeben müssen.
  GroupShield hilft die von Ihren Microsoft® Exchange-Servern benötigten Übertragungs- und Speicherkapazitäten frei zu halten, indem jeder E-Mail beim Scannen ein Spamfaktor zugewiesen wird und die für diese Nachrichten konfigurierte Aktion durchgeführt wird.

- *Anti-Phishing* — GroupShield kann E-Mail-Nachrichten mit Phishing-Hinweisen erkennen, wobei auf betrügerische Weise versucht wird, an persönliche Daten zu gelangen. In der Regel werden die Empfänger von Phishing-E-Mails dazu aufgefordert, auf einen Link in der E-Mail zu klicken, um ihre Kontakt- oder Kreditkartendaten oder andere persönliche Informationen zu bestätigen oder zu aktualisieren.

- *Inhaltfilterung* — GroupShield ermöglicht das Scannen von Inhalt/Text in folgenden Elementen:
  - Betreffzeile der E-Mail
  - Haupttext der E-Mail
  - Anlage der E-Mail
- *Dateifilterung* — GroupShield scannt eine E-Mail-Anlage abhängig von Dateiname, Dateityp und Dateigröße dieser Anlage.
- *Enterprise-Rollout, Verwaltung, Aktualisierung und Berichterstellung mit McAfee® ePolicy Orchestrator und McAfee® ProtectionPilot* — GroupShield ist in McAfee® ePolicy Orchestrator und McAfee® ProtectionPilot integriert und bietet eine zentrale Methode für den Rollout, die Verwaltung und Aktualisierung von Ihrer GroupShield-Software in Ihrem Microsoft® Exchange-System. Die Fähigkeit zur zentralen Verwaltung einer unternehmensweiten Implementierung der GroupShield-Software reduziert den Zeitaufwand für Verwaltung und Aktualisierung des Systems.

Was ist neu?

- *Neue webbasierte Benutzeroberfläche* — GroupShield für Exchange stellt eine benutzerfreundliche, webbasierte Oberfläche auf DHTML-Basis zur Verfügung. Zum Aufrufen klicken Sie einfach auf **Start** | **Programme** | **McAfee** | **GroupShield für Exchange** | **GroupShield für Exchange (Web)**.
- *Richtlinienverwaltung* — Die Menüoption **Richtlinien-Manager** listet die unterschiedlichen Richtlinien auf, die Sie in GroupShield einrichten und verwalten können. Sie können verschiedene Richtlinien/Aktionen festlegen, die ermitteln, welche Aktionen bei welchen Bedrohungen ausgeführt werden sollen. Detaillierte Informationen zur Richtlinienverwaltung finden Sie im Kapitel *Richtlinien-Manager auf Seite 117*.
- *Anti-Phishing-Funktion* — GroupShield für Exchange kann E-Mail-Nachrichten mit Phishing-Hinweisen erkennen, wobei auf betrügerische Weise versucht wird, an persönliche Daten zu gelangen.
- *Erkennungsfunktionen für Komprimierungsprogramme und potenziell unerwünschte Programme* — GroupShield für Exchange kann Komprimierungsprogramme erkennen, die den Originalcode einer ausführbaren Datei komprimieren und verschlüsseln.
  Außerdem werden potenziell unerwünschte Programmen entdeckt. Dabei handelt es sich um Softwareprogramme von rechtmäßigen Unternehmen, welche den Sicherheitsstatus oder das Datenschutzniveau des Computers, auf dem sie installiert sind, verändern können.

- *Verbesserte Anti-Spam-Funktionalität* — GroupShield für Exchange kann Spam- und unerwünschte Massen-E-Mails erkennen, die an mehrere Empfänger ohne deren Anforderung gesendet wurden. Jeder E-Mail wird ein „Spamfaktor" zugewiesen. Sie können festlegen, dass Nachrichten, die einen bestimmten Faktor übersteigen, blockiert werden.

- *Verbesserte Hintergrundscan-Optionen* — GroupShield bietet bei Exchange Server 2007 verbesserte Optionen für Hintergrundscans. Bei dieser Art des Scannens werden nicht alle E-Mails bei Zugriff gescannt. Dies verringert die Arbeitslast des Scanners. Weitere Informationen finden Sie im Unterthema *Für Exchange Server 2007 auf Seite 184*.

- *Zentrale Einstellungen für Scanner und Filterregeln sowie erweiterte Warneinstellungen* — Unter **Scanner** können Sie scannerbezogene Einstellungen konfigurieren, die von einer Richtlinie beim Scannen der Elemente angewendet werden können.
  Unter **Dateifilterregeln** können Sie Regeln für Dateinamen, -typ und -größe festlegen. Mit dem Warnungseditor können Sie den Text einer Warnmeldung über die Menüs **Stil**, **Schriftart**, **Größe** und **Token** bearbeiten.

- *Zeitbasiertes Scannen und Aktionen* — GroupShield für Exchange ermöglicht das Scannen von E-Mails zu gewünschten Zeiten oder in regelmäßigen Abständen. Sie können regelmäßige Scanvorgänge planen, wenn diese Ihre Arbeit nicht beeinträchtigen und die Serveraktivitäten vergleichsweise gering sind.

- Inhaltsscans und Filterung nach echtem Dateityp bei ® Office 2007-Dateiformaten

- *Filter für kennwortgeschützte ZIP-Dateien* — Weitere Informationen zu diesem Filter finden Sie unter *Kennwortgeschützte Dateien auf Seite 154*.

- *Filter für geschützten Inhalt (kennwortgeschützte Microsoft® Office-Dateien)* — Weitere Informationen zu diesem Filter finden Sie unter *Geschützter Inhalt auf Seite 150*.

- *Unterstützung von N+1-Clustern* — Weitere Informationen finden Sie unter *Single Copy Cluster (SCC, N+1-Clusterkonfiguration) unter Exchange Server 2003 und 2007 auf Seite 35*.

- *Verbessertes MIME-Scannen* — MIME (Multipurpose Internet Mail Extensions) ist ein Kommunikationsstandard, der die Übertragung von Nicht-ASCII-Formaten über Protokolle (wie SMTP) gestattet, die nur 7-Bit-ASCII-Zeichen unterstützen. In GroupShield können Sie festlegen, wie mit diesen MIME-Nachrichten zu verfahren ist.

- *Schutz vor Pufferüberlauf mit VirusScan Enterprise Version 8.5i* — Ein Pufferüberlauf ist eine nicht normale Bedingung, bei der ein Prozess versucht, Daten über die Grenzen eines festgelegten Puffers hinaus zu speichern. Dieser Prozess verursacht, dass benachbarte Speicherorte überschrieben werden. Die Aktivierung der Option **Schutz vor Pufferüberläufen** verhindert diese Bedingung. GroupShield stellt den Schutz vor Pufferüberläufen zur Verfügung. Weitere Informationen finden Sie unter *Schutz vor Pufferüberläufen auf Seite 31*

  Der Schutz vor Pufferüberläufen ist nur auf 32-Bit-Plattformen (und nicht auf 64-Bit-Plattformen) mit Exchange Server 2003 verfügbar.

- *Verbesserte Quarantäneverwaltung*
  - *Lokale Quarantäneverwaltung* — Erkannte Elemente können isoliert werden. Sie können die lokale Datenbank als Repository für isolierte E-Mail-Nachrichten festlegen. Außerdem können Sie die Wartungseinstellungen für die lokale Quarantäne-Datenbank konfigurieren.
  - *Isolieren mit McAfee Quarantine Manager Version 4.1 oder 4.1.1* — Sie können den McAfee Quarantine Manager auf einem anderen Server als Repository für das Isolieren infizierter E-Mails angeben. So bleibt Ihr Exchange Server vor Viren geschützt.
- Integration in:
  - *McAfee ePolicy Orchestrator Version 3.6 und 4.0* — stellt die gemeinsame Steuerungszentrale für alle im Unternehmen eingesetzten McAfee-Antivirusprodukte dar, in der Sie Antivirenrichtlinien verwalten und Berichte zu Antivirusereignissen und Virusaktivitäten einsehen können. Weitere Informationen finden Sie in den Kapiteln *Integrieren in ePolicy Orchestrator 3.6 auf Seite 49* und *Integrieren in ePolicy Orchestrator 4.0 auf Seite 67*.
  - *McAfee ProtectionPilot Version 1.5 und höher* — bietet eine Sicherheitsverwaltung, die Netzwerkadministratoren, die für bis zu 500 Computern zuständig sind, eine einfachere Antivirusverwaltung ermöglicht. Die Verwaltungsaufgaben umfassen die Bereitstellung (Senden und Installieren) von Virenschutzprodukten, die Konfiguration von Produkteinstellungen und die regelmäßige Aktualisierung dieser Produkte. Weitere Informationen finden Sie in Kapitel *Integrieren in ProtectionPilot 1.5 auf Seite 83*.
  - *Antivirus-Modul 5200* — bietet verbesserte und aktuelle Erkennung von Komprimierungsprogrammen und potenziell unerwünschten Programmen sowie verbesserten Emulator mit flexiblen Methoden.

- Koexistenz mit:
  - McAfee VirusScan Enterprise Version 8.0 und höher.
  - McAfee Host Intrusion Prevention Agent.
- *Automatische Aktualisierung von Virendefinitionen (V2API DATs), ExtraDATs, Antivirus-Modul, Anti-Spam-Modul und Anti-Spam-Regeln* — McAfee Security stellt in regelmäßigen Abständen Virusdefinitionsdateien (DAT) bereit sowie Virusscanmodul, Anti-Spam-Modul und Regeln zur Erkennung und Beseitigung der neuesten Bedrohungen.

  GroupShield verwendet die neue Version der Antivirus-DATs und des Antivirusmoduls (V2API). Dies verbessert die Erkennung der neuesten Viren und Bedrohungen.

- *Produktaktualisierung mit der ausführbaren SuperDAT-Datei, Version 2.2* — GroupShield schützt Ihren Server vor Viren, Trojanern, Spam, Phishing und potenziell unerwünschten Programmen durch regelmäßige Produktaktualisierung mithilfe der ausführbaren SuperDAT-Datei.
- *Produkteigene Berichte* — GroupShield erzeugt Statusberichte und Grafikberichte zur Anzeige von Informationen zu den erkannten Elementen.
- *Antivirus-Stamping-Mechanismus auf einem ® Exchange Server 2007 mit Edge- oder Hub-Serverfunktion* — Der McAfee®-Transport-Scanner weist der Kopfzeile einer E-Mail nach dem Scannen einen Stempel zu. So wird ein erneutes Scannen der Nachricht durch VSAPI verhindert.
- *Richtungsbasiertes Scannen* — GroupShield unterstützt richtungsbasiertes Scannen. Mithilfe des McAfee®-Transport-Scanners werden eingehende, ausgehende sowie interne E-Mails gescannt.
- *Schwarze und weiße Benutzer- und Serverlisten unter Verwendung des McAfee Quarantine Manager, Version 4.1* — Weitere Informationen finden Sie unter *Aktualisieren von schwarzen und weiße Listen auf Seite 44*.
- *Integration in SuperDAT Manager Version 2.2* — SuperDAT Manager 2.2 unterstützt die Aktualisierung von DAT und Modul für die GroupShield-Software.
- *Integration in McAfee Common Management Agent (CMA) Version 3.6 und höher* — Mithilfe der CMA-Komponente können Sie GroupShield verwalten und im Rahmen der Kerninstallation Produktaktualisierungen und geplante Aufgaben durchführen sowie Ereignisberichte erstellen.

Nicht unterstützte Funktionen

- Integration in Serveranwendungen für schwarze und weiße Listen, die zusammen mit GroupShield für Exchange, Version 6.x, installiert wurden.
- Integration in Outbreak Manager (OBM).
- Integration in Alert Manager (AM).
- Integration in ProtectionPilot 1.1.
- Integration in ePolicy Orchestrator 3.5.x.
- Integration in Exchange Server 2000.
- Integration in Common Management Agent 3.5.x.
- Integration in McAfee AutoUpdate Architect 1.x.

Verwenden dieses Handbuchs

Dieses Handbuch beschreibt schrittweise den Installationsprozess von McAfee GroupShield™ 7.0 für Microsoft® Exchange 2003 und 2007. Außerdem finden Sie hier eine detaillierte Beschreibung der Software. Folgende Themen werden behandelt:

- *Vor dem Installieren* — Szenarien vor der Installation und Systemanforderungen.
- *Installieren der Software* — Zugreifen auf und Installieren von GroupShield.
- *Post-Installation und Wartung* — Testen der GroupShield-Installation, Antiviruskomponente, Anti-Spam-Komponente und Testen mithilfe von McAfee Virtual Technician. Isolieren mithilfe des McAfee Quarantine Manager, Modifizieren, Reparieren, Wiederherstellen und Deinstallieren der Software.
- *Integrieren in ePolicy Orchestrator 3.6* — Testen der GroupShield-Integration in ePolicy Orchestrator Version 3.6.
- *Integrieren in ePolicy Orchestrator 4.0* — Testen der GroupShield-Integration in ePolicy Orchestrator Version 4.0.
- *Integrieren in ProtectionPilot 1.5* — Testen der GroupShield-Integration in ProtectionPilot.
- *Erste Schritte in der Benutzeroberfläche* — Verwenden von GroupShield für Microsoft® Exchange Server 2003/2007, Abrufen detaillierter Informationen über das Dashboard, erkannte Elemente, Richtlinien-Manager sowie Einstellungen und Diagnose.

Zielgruppe

Dieses Handbuch wurde für Netzwerkadministratoren zusammengestellt, die für das Antiviren-Programm ihres Unternehmens verantwortlich sind.

Konventionen

In diesem Handbuch werden folgende Konventionen verwendet:

Schmalfett	Alle Wörter aus Benutzeroberflächen, einschließlich Optionen, Menüs, Schaltflächen und Dialogfeldnamen. **Beispiel:** Geben Sie **Benutzernamen** und **Kennwort** des betreffenden Kontos ein.

`Courier`	Der Pfad eines Ordners oder Programms; Text, der für eine genaue Eingabe des Anwenders steht (z. B. ein Befehl in der Befehlszeile).
	Beispiele:
	Die standardmäßige Adresse des Programms lautet:
	`C:\Programme\McAfee\EPO\3.6.0`
	Führen Sie diesen Befehl auf dem Client-Computer aus:
	`scan --help`

Kursiv	Betonung, Einführung eines neuen Begriffs; Namen von Produktdokumentationen und Themen (Überschriften) in den Handbüchern. **Beispiel:** Weitere Informationen finden Sie im *VirusScan Enterprise-Produkthandbuch*.
Blau	Eine Webadresse (URL) und/oder aktive Links. **Beispiel:** Besuchen Sie die Website von McAfee unter: `http://www.mcafee.com`
<BEGRIFF>	In eckigen Klammern stehen allgemeine Begriffe. **Beispiel:** Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf <SERVER>.
	Hinweis: Zusätzliche Informationen, beispielsweise eine alternative Methode zum Ausführen des gleichen Befehls.
	Tipp: Vorschläge für bewährte Vorgehensweisen und Empfehlungen von McAfee zu den Themen Vermeidung von Bedrohungen, Leistung und Effizienz.
	Achtung: Wichtiger Hinweis zum Schutz von Benutzer, Computersystem, Unternehmen, Softwareinstallation oder Daten.
	Warnung: Wichtiger Hinweis zum Schutz von Benutzern vor körperlichen Schäden durch die Verwendung eines Hardwareprodukts.

Abrufen von Produktinformationen

Sofern nicht anders angegeben, wird die Produktdokumentation im Adobe Acrobat PDF-Format zur Verfügung gestellt, entweder in Form einer Produkt-CD oder über die McAfee-Download-Site.

Standarddokumentation

Benutzerhandbuch — Systemanforderungen und Anweisungen zum Installieren und Starten der Software. Vorstellung des Produkts und seiner Funktionen, ausführliche Anweisungen für die Softwarekonfiguration, Informationen zu Bereitstellung, sich wiederholenden Tasks und Vorgehensweisen.

Hilfe — Hochwertige und detaillierte Informationen, die in der Software selbst zur Verfügung stehen: Menü **Hilfe** und/oder Schaltfläche **Hilfe** für Unterstützung auf Seitenebene, Kontextmenü für punktgenaue Unterstützung (*Was ist das?*).

Versionshinweise — *Infodatei*. Produktinformationen, behobene Fehler, etwaige bekannte Probleme, in letzter Minute am Produkt oder an diesem Handbuch vorgenommene Ergänzungen und Änderungen.

Kontaktinformationen

Virenschutz-Center: McAfee Avert® Labs http://www.mcafee.com/us/threat_center/default.asp

Avert Labs-Bedrohungsbibliothek
http://vil.nai.com

Avert Labs WebImmune und Muster übermitteln *(Anmeldeinformationen erforderlich)*
https://www.webimmune.net/default.asp

Avert Labs DAT-Benachrichtigungsdienst
http://vil.nai.com/vil/signup_DAT_notification.aspx

Download-Site http://www.mcafee.com/us/downloads/

Produkt-Upgrades *(Gültige Lizenznummer erforderlich)*

Sicherheitsaktualisierungen (DATs, Modul)

HotFix- und Patch-Veröffentlichungen

- **Für Sicherheitsschwachstellen** *(öffentlich verfügbar)*
- **Für Produkte** *(ServicePortal-Konto und gültige Lizenznummer erforderlich)*

Produktevaluierung

Beta-Programm von McAfee

Technischer Support http://www.mcafee.com/us/support/

Suchen in der KnowledgeBase
http://knowledge.mcafee.com/

McAfee ServicePortal des technisches Supports *(Anmeldeinformationen erforderlich)*
https://mysupport.mcafee.com/eservice_enu/start.swe

Kundendienst

Web
http://www.mcafee.com/us/support/index.html
http://www.mcafee.com/us/about/contact/index.html

Telefon – USA, Kanada und Lateinamerika (gebührenfrei):
+1-888-VIRUS NO oder **+1-888-847-8766** Montag-Freitag, 8.00-20.00 Uhr, Central Time

Professional Services

Großunternehmen: http://www.mcafee.com/us/enterprise/services/index.html

Kleine und mittlere Unternehmen: http://www.mcafee.com/us/smb/services/index.html

2 Vor dem Installieren

Dieses Kapitel enthält wichtige Informationen zur Vorbereitung der Installation von GroupShield für Exchange 7.0. Folgende Themen werden behandelt:

- *Szenarien vor der Installation*
- *Systemvoraussetzungen*

Szenarien vor der Installation

Sie MÜSSEN sich bei Microsoft® Windows als Domänenadministrator anmelden. Dadurch erhalten Sie die zum Installieren von GroupShield benötigten Rechte und Berechtigungen.

Vor der Installation von GroupShield:

- Stellen Sie sicher, dass Microsoft® Exchange Server 2003/2007 auf dem Installationsserver installiert ist.
- Deinstallieren Sie manuell alle älteren GroupShield-Softwareversionen als 6.0.2.

GroupShield für Exchange 7.0 unterstützt die automatische Aktualisierung der Software von Version 6.0.2 und höher.

- Deinstallieren Sie SpamKiller für Exchange mithilfe der Windows-Funktion **Software**.

GroupShield für Exchange 7.0 unterstützt keine Aktualisierung der SpamKiller-Software.

Installationsarten

GroupShield kann wie folgt auf Microsoft® Exchange Server 2003/2007 installiert werden:

- *Standardinstallation*
- *Hintergrundinstallation*
- *Cluster-Installation*

Standardinstallation

Sie können die McAfee® GroupShield-Software auf Microsoft® Exchange Server 2003/2007 installieren. Schrittweise Anleitungen finden Sie unter *Installieren von GroupShield für Microsoft® Exchange Server 2003/2007 auf Seite 26*.

Hintergrundinstallation

Sie können die McAfee® GroupShield-Software auf Microsoft® Exchange Server 2003/2007 installieren, ohne dass eine Benutzeraktion erforderlich ist. Dies wird auch als unbeaufsichtigte Installation bezeichnet. Schrittweise Anleitungen finden Sie unter *Hintergrundinstallation auf Seite 32*.

Cluster-Installation

Sie können die McAfee® GroupShield-Software auf Microsoft® Exchange Server 2003/2007 in einer Cluster-Umgebung installieren. Schrittweise Anleitungen finden Sie unter *Konfigurieren von GroupShield in einer Clusterumgebung auf Seite 34*.

Systemanforderungen

Stellen Sie vor der Installation von GroupShield sicher, dass Ihr Server folgende Anforderungen erfüllt:

Tabelle 2-1 Systemanforderungen

Prozessor	■ Auf Intel x64-Architektur basierter Prozessor mit Unterstützung der Intel EM64T-Architektur (Intel Extended Memory 64 Technology) ■ Auf AMD x64-Architektur basierter Prozessor mit AMD 64-Bit-Technologie ■ Auf Intel x86-Architektur basierter Prozessor (nur bei Exchange Server 2003)
Arbeitsspeicher	■ Mindestanforderung: 512 MB ■ Empfohlen: 1 GB
Verfügbarer Festplattenspeicher	■ Mindestanforderung: 740 MB
Betriebssystem	■ Windows 2000 Advanced Server mit Service Pack 4 ■ Windows 2003 Standard/Enterprise Server (32-Bit) ■ Windows 2003 Standard/Enterprise Server R2 (32-Bit) ■ Windows 2003 Standard/Enterprise Server (64-Bit) ■ Windows 2003 Small Business Server (32-Bit) ■ Windows 2003 Datacenter Server (32-Bit) ■ Windows 2003 Datacenter Server (64-Bit) **Hinweis:** Informationen zu Service Packs finden Sie in den Versionshinweisen unter den Anforderungen für Windows-Service Packs.
Unterstützte Exchange Server	■ Microsoft® Exchange Server 2003 mit Service Pack 2 ■ Microsoft® Exchange Server 2007
Unterstützte Browser	■ Microsoft® Internet Explorer Version 6 und höher ■ Netscape Navigator Version 9.0 ■ Mozilla Version 2.0
Bildschirmauflösung	1024 x 768 Setzen Sie die Auflösung auf 24 Bit oder höher, um eine optimale Anzeige zu erreichen.
Allgemein	Ein CD-ROM-Laufwerk (bei Installation von CD) oder ein Internetzugang (bei Installation über die McAfee-Download-Website)

3 Installieren der Software

Die Installation der GroupShield-Software umfasst die folgenden Themen:

- *Zugreifen auf die Software*
- *In der Software enthaltene Komponenten*
- *Installieren von GroupShield für Microsoft® Exchange Server 2003/2007*
- *Installieren zusätzlicher Komponenten*
- *Hintergrundinstallation*
- *Konfigurieren von GroupShield in einer Clusterumgebung*
- *Aktualisieren von GroupShield von v6.0.2 oder höher*

Zugreifen auf die Software

McAfee stellt GroupShield für Exchange auf zwei Arten bereit:

- Als eine archivierte Datei, die Sie von der McAfee-Website oder anderen elektronischen Diensten herunterladen.
- Auf der Total Virus Defense (TVD)-CD, der Active Virus Defense (AVD)-CD oder der Produktsuite-CD.

Nachdem Sie die Archivdatei heruntergeladen und die TVD- oder AVD-Installations-CD in das CD-ROM-Laufwerk eingelegt haben, werden Sie schrittweise durch die Installation geführt. Die Installationsschritte sind für jeden Distributionstyp gleich.

Um GroupShield für Microsoft® Exchange Server 2003/2007 zu installieren, zu verwalten, zu entfernen oder zu aktualisieren müssen Sie über Administratorrechte verfügen.

In der Software enthaltene Komponenten

GroupShield für Exchange verfügt über die folgenden Komponenten im Installationsprogramm, die separat installiert werden können.

- **McAfee GroupShield für Exchange 7.0**
- **Schutz vor Pufferüberläufen**
- **McAfee Anti-Spam für GroupShield**

Die Option **McAfee GroupShield für Exchange 7.0** wird standardmäßig ausgewählt. Wenn Sie zusätzliche Komponenten installieren möchten, müssen Sie diese während der Installation auswählen.

McAfee® GroupShield™ für Microsoft® Exchange Server 2003/2007 enthält keine Aktualisierung für die McAfee® SpamKiller für Exchange-Installation. Sie sollten McAfee® SpamKiller für Exchange manuell deinstallieren, bevor Sie GroupShield für Exchange 7.0 installieren.

Installieren von GroupShield für Microsoft® Exchange Server 2003/2007

1. Melden Sie sich mit einem Administratorkonto bei Microsoft® Exchange Server 2003/2007 an.
2. Erstellen Sie ein temporäres Verzeichnis im Netzwerk oder auf dem lokalen Laufwerk.
3. Für die Installation führen Sie einen der folgenden Schritte aus, abhängig davon, wie Sie die Software erhalten haben:
   - Legen Sie die CD-ROM in das Laufwerk des Computers ein, und kopieren Sie die Installationsdateien in das erstellte temporäre Verzeichnis.
   - Laden Sie das ZIP-Archiv herunter, und extrahieren Sie die Dateien in ein temporäres Verzeichnis.

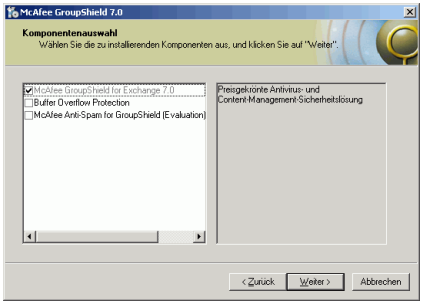
4 Wechseln Sie im Windows Explorer zu dem Ordner, in den Sie die Installationsdateien kopiert haben, und doppelklicken Sie auf **SETUP.EXE**. Das Setupdialogfeld **GroupShield für Exchange** wird angezeigt.

Abbildung 3-1 McAfee GroupShield für Exchange – Willkommen

McAfee GroupShield 7.0
Willkommen bei der Installation von McAfeeGroupShield für Exchange
Sie sollten unbedingt alle Windows-Programme beenden, bevor Sie dieses Setup-Programm ausführen.
Klicken Sie auf "Abbrechen", um das Setup-Programm zu beenden, und schließen Sie dann alle aktiven Programme.
Klicken Sie auf "Weiter", um die Installation fortzusetzen.
WARNUNG: Dieses Programm ist weltweit urheberrechtlich geschützt. Unautorisierte Vervielfältigung oder Weitergabe dieses Programmes oder von Teilen dieses Programms wird zivil- und strafrechtlich verfolgt werden. Copyright (C) 2007 McAfee, Inc. Alle Rechte vorbehalten.
< Zurück
Weiter >
Abbrechen

5 Klicken Sie auf **Weiter**. Das Dialogfeld **Komponentenauswahl** mit den verfügbaren Softwarekomponenten wird angezeigt.

Abbildung 3-2 McAfee GroupShield für Exchange – Komponentenauswahl


McAfee GroupShield 7.0
Komponentenauswahl
Wählen Sie die zu installierenden Komponenten aus, und klicken Sie auf "Weiter".
McAfee GroupShield for Exchange 7.0
Buffer Overflow Protection
McAfee Anti-Spam for GroupShield (Evaluation)
Preisgekrönte Antivirus- und Content-Management-Sicherheitslösung
< Zurück
Weiter >
Abbrechen

- Die Option **McAfee GroupShield für Exchange 7.0** wird standardmäßig ausgewählt.
- **Schutz vor Pufferüberläufen** bietet Schutz über McAfee VirusScan Enterprise Version 8.5i vor Host-Eindringung und einem damit verbundenen Pufferüberlauf.

Schutz vor Pufferüberlauf wird auf 64-Bit-Plattformen nicht unterstützt.

- **McAfee Anti-Spam für GroupShield (Testversion)** bietet Filter zum Blockieren von Spam- und Phishing-E-Mails.

Die Anti-Spam- und Anti-Phishing-Funktionalität ist nur verfügbar, wenn Sie bei der Installation die Komponente **McAfee Anti-Spam für GroupShield** ausgewählt haben. Damit dieses Add-On im lizenzierten Modus ausgeführt wird, muss es zuvor aktiviert werden.

6 Wählen Sie die Softwarekomponenten aus, die Sie installieren möchten, und klicken Sie auf **Nächste**.

Wenn der **Installations-Assistent** bei der Vorbereitung der Installation erkennt, dass auf Ihrem Computer noch Programme geöffnet sind, werden Sie in einem Dialogfeld zum Schließen der Programme aufgefordert.

7 Anschließend wird das Dialogfeld **Endbenutzervertrag** angezeigt. Wählen Sie dort aus den entsprechenden Dropdown-Menüs die Optionen **Ablauftyp der Lizenz** und **Ort des Kaufs und der Verwendung** auswählen aus.

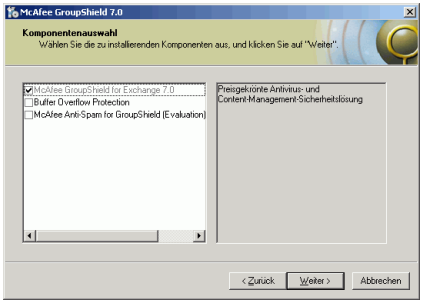
8 Klicken Sie auf **Ich akzeptiere die Bedingungen des Lizenzvertrags** und dann auf **OK**, um das Dialogfeld **Zielordner** anzuzeigen.

9 Klicken Sie auf **Durchsuchen**, um einen anderen Ordner auszuwählen, oder auf **Nächste**, wenn Sie die Software im Standardverzeichnis installieren möchten. Das Dialogfeld **Installationstyp auswählen** wird angezeigt.

10 Wählen Sie eine der folgenden Installationsoptionen aus:

- **Standard** — Die gängigsten Anwendungsfunktionen werden installiert. Diese Option ist für die meisten Benutzer geeignet.
- **Vollständig** — Installiert alle Anwendungsfunktionen.
- **Benutzerdefiniert** — Installiert vom Benutzer ausgewählte Anwendungsfunktionen. Empfohlen für erfahrene Benutzer.

Abbildung 3-3 McAfee GroupShield für Exchange – Installationstyp auswählen


McAfee GroupShield 7.0
Komponentenauswahl
Wählen Sie die zu installierenden Komponenten aus, und klicken Sie auf 'Weiter'.
McAfee GroupShield for Exchange 7.0
Buffer Overflow Protection
McAfee Anti-Spam for GroupShield (Evaluation)
Preisgekrönte Antivirus- und Content-Management-Sicherheitslösung
< Zurück
Weiter >
Abbrechen

11 Klicken Sie auf **Weiter**. Das Dialogfeld **Bereit zum Installieren der Anwendung** wird angezeigt. Wählen Sie **Verknüpfung erstellen**, um eine Verknüpfung auf dem Desktop zu erstellen.

12 Klicken Sie auf **Weiter**, um das Dialogfeld **Systemaktualisierung** anzuzeigen. In einer Statusanzeige werden die Funktionen angezeigt, die zurzeit kopiert und installiert werden. Klicken Sie nach Abschluss der Installation auf **Fertig stellen**, um die Installation von GroupShield für Exchange abzuschließen.

13 Nach der erfolgreichen Durchführung der Installation wird folgendes Menü unter **Start | Programme | McAfee | GroupShield für Exchange** angezeigt:

- **GroupShield für Exchange (Web)**
- **SiteList Editor**
- **GroupShield für Exchange**
- **GroupShield für Exchange-Zugriffssteuerung**

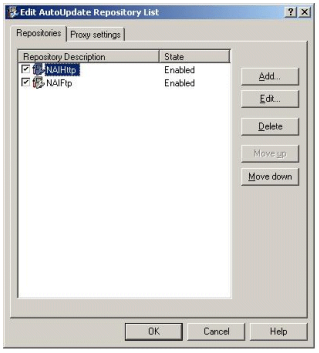
Die Option **GroupShield für Exchange (Web)** wird nur bei Auswahl des Installationstyps **Vollständig** im Menü angezeigt.

SiteList Editor

Mit dieser neuen Softwarefunktionen können Sie die List der zur Aktualisierung konfigurierten Sites anzeigen. Die Benutzeroberfläche weist Ähnlichkeiten mit derjenigen von McAfee VirusScan Enterprise auf.

Diese Anwendung ändert die Datei **sitelist.xml** auf dem aktuellen Computer. **EditSiteList.exe** ist das Tool zum Bearbeiten der Datei **sitelist.xml**.

Abbildung 3-4 SiteList Editor

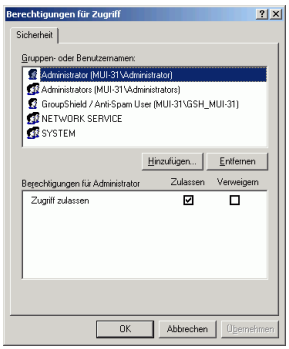


GroupShield für Exchange-Zugriffsteuerung

Die Zugriffssteuerung wird verwendet, um den Benutzerzugriff auf die GroupShield-Software zu beschränken. Sie können die Verwaltung der Zugriffssteuerung vereinfachen, indem Sie eine oder mehrere administrative Bentuzergruppen verwenden und für jede Gruppe die gewünschten Berechtigungen festlegen. Fügen Sie dann die einzelnen Benutzer den Benutzergruppen hinzu, um ihnen die jeweiligen Berechtigungen zu gewähren.

Berechtigungen können jedem Objekt im Verzeichnis oder auf dem lokalen Computer zugewiesen werden. Die meisten Berechtigungen gelten jedoch Gruppen anstelle von einzelnen Benutzern. Die Verwaltung von Berechtigungen für die Software wird somit erheblich vereinfacht.

Abbildung 3-5 Zugriffssteuerung



Installieren von zusätzlichen Komponenten

Nachdem der Assistent die eigentliche Installation von abgeschlossen hat, können Sie noch die folgenden zusätzlichen Komponenten auswählen und installieren:

- **Schutz vor Pufferüberläufen**
- **McAfee Anti-Spam für GroupShield**

Die Komponente **McAfee GroupShield für Exchange 7.0** wird standardmäßig ausgewählt. Um die zusätzlichen Softwarekomponenten zu installieren, müssen Sie sie im Installer auswählen. Zur Aktivierung von McAfee Anti-Spam für GroupShield ist ein Lizenzschlüssel erforderlich.

Schutz vor Pufferüberläufen

Pufferüberläufe stellen eine Angriffstechnik dar, mit der ein Softwareentwicklungsfehler in einer Anwendung oder einem Prozess ausgenutzt wird, um die Ausführung von Code auf dem Computer zu erzwingen. Anwendungen verfügen über Puffer zum Speichern von Daten in einer festgelegten Größe. Wenn ein Angreifer zu viele Daten oder Code an einen dieser Puffer sendet, läuft der Puffer über. Der Comptuer führt dann den übergelaufenen Code als ein Programm aus.
Da die Codeausführung im Sicherheitskontext der Anwendung stattfindet (häufig auf administrativer Ebene mit einem hohen Grad an Berechtigungen), können Eindringlinge Befehle ausführen, die normalerweise schwer zugänglich sind. Eine Angreifer kann diese Schwachstelle ausnutzen, um beliebigen Hacker-Code auf dem Computer auszuführen und die Sicherheit des Systems und die Datenintegrität lahm zu legen.

Schutz vor Pufferüberläufen verhindert die Ausnutzung von Pufferüberläufen zur Ausführung von beliebigen Code auf Ihrem Computer. Mit dieser Funktion werden API-Aufrufe im Benutzermodus überwacht und neu organisiert, wenn diese das Ergebnis eines Pufferüberlaufs darstellen.

GroupShield für Exchange verwendet die Funktion zum Schutz vor Pufferüberläufen von VirusScan Enterprise, um die folgenden Prozesse zu schützen:

- RPCServ.exe
- PrfCtrs.exe
- RunScheduled.exe
- SAFeService.exe
- SDEDIT.exe
- StandaloneUI.exe

Aktivieren der Funktion zum Schutz vor Pufferüberläufen:

Wechseln Sie im Windows Explorer zu dem Ordner, in den Sie die Installationsdateien kopiert haben, und doppelklicken Sie auf **BOPActivation.EXE**.

Weitere Informationen zum Schutz vor Pufferüberläufen finden Sie im *Benutzerhandbuch für VirusScan Enterprise v 8.5*.

Installieren von McAfee Anti-Spam für GroupShield

Die Anti-Spam- und Anti-Phishing-Funktionalität ist nur verfügbar, wenn Sie bei der Installation die Komponente McAfee Anti-Spam für GroupShield ausgewählt haben. Damit dieses Add-On im lizenzierten Modus ausgeführt wird, muss es zuvor aktiviert werden.

1. Wenn Sie im Dialogfeld **Komponentenauswahl** die Option **McAfee Anti-Spam für GroupShield** ausgewählt haben, wird das Dialogfeld **Add-On-Paket** geöffnet.
2. Klicken Sie auf **Weiter**. Anschließend wird das Dialogfeld mit dem **Endbenutzervertrag** angezeigt. Wählen Sie die Option **Ort des Kaufs und der Verwendung** aus dem Dropdown-Menü aus.
3. Klicken Sie auf **Weiter**, um die Anti-Spam-Funktion zu installieren. Schließen Sie anschließend die Add-On-Installation ab, indem Sie auf **Fertig stellen** klicken.

Hintergrundinstallation

Die Installation von GroupShield für Exchange wird von MSI ausgeführt. Sie können die von MSI verwendeten Eigenschaften einstellen. Dazu bearbeiten Sie die Datei `SILENT.INI` oder übermitteln die Eigenschaften über die Befehlszeile direkt an MSI.

Mit einer Hintergrundinstallation ist die Installation von GroupShield für Exchange unter Microsoft® Windows zu einem passenden Zeitpunkt möglich. Ein weiterer Vorteil der Hintergrundinstallation ist der im Vergleich zu einer manuellen Installation weitgehend automatisierte Installationsvorgang.

Stellen Sie vor der Installation sicher, dass der Windows-Netzwerkanmeldungsdienst auf dem Windows-Server mit Domänen-Controllern ausgeführt wird.

Mit der Hintergrundinstallation können Sie keine Komponenten hinzufügen oder entfernen und keine Reparatur ausführen.

Installieren von GroupShield für Exchange im Hintergrund

1. Melden Sie sich mit einem Administratorkonto bei Microsoft® Exchange Server 2003/2007 an.
2. Erstellen Sie ein temporäres Verzeichnis im Netzwerk oder auf dem lokalen Laufwerk.

3 Für die Installation führen Sie einen der folgenden Schritte aus, abhängig davon, wie Sie die Software erhalten haben:

- Legen Sie die CD-ROM in das Laufwerk des Computers ein, und kopieren Sie die Installationsdateien in das erstellte temporäre Verzeichnis.
- Laden Sie das ZIP-Archiv herunter, und extrahieren Sie die Datei in das temporäre Verzeichnis.

4 Wechseln Sie an der Befehlszeile in das temporäre Verzeichnis, in das Sie die Installationsdateien extrahiert haben.

5 Stellen Sie sicher, dass sich die Datei `GROUPSHIELD.MSI` im temporären Ordner befindet.

6 Geben Sie `MSIEXEC /I <Full Path of the MSI> /QN` ein, und drücken Sie die EINGABETASTE.

Temporäres Verzeichnis = C:\GSE7

```
MSIEXEC /I C:\GSE7\GROUPSHIELD.MSI /QN
```

7 So installieren Sie ein Verzeichnis in einen **Benutzerdefinierten** Ordner und protokollieren die Installation:

`MSIEXEC /I <MSI path> INSTALLDIR=<Installationsverzeichnis>` und drücken Sie die EINGABETASTE.

Installationsverzeichnis = C:\GSE7INSTALL

```
MSIEXEC /I C:\GSE7\GROUPSHIELD.MSI INSTALLDIR=C:\GSE7INSTALL /QN
MSIEXEC /I <MSI-Pfad> INSTALLDIR=<Installationsverzeichnis> /l*
<Name und Pfad von Protokolldatei>
MSIEXEC /I C:\GSE7\GROUPSHIELD.MSI INSTALLDIR=C:\GSE7INSTALL /l*
C:\GSE7\GSELOG.TXT /QN
```

Nach der erfolgreichen Durchführung der Installation wird folgendes Menü unter **Start** | **Programme** | **McAfee** | **GroupShield für Exchange** angezeigt:

- **GroupShield für Exchange**
- **GroupShield für Exchange-Zugriffssteuerung**
- **SiteList Editor**

Bei der Installation im Hintergrund wird lediglich die GroupShield-Software auf dem Server installiert. Wenn Sie zusätzliche Komponenten wie Anti-Spam für GroupShield und die Funktion zum Schutz vor Pufferüberläufen installieren möchten, führen Sie die jeweiligen Setupdateien manuell aus.

Konfigurieren von GroupShield in einer Clusterumgebung

In diesem Abschnitt werden die Schritte für die Konfiguration von GroupShield in einer Clusterumgebung beschrieben.

GroupShield 7.0 wird auf einem *Microsoft® Cluster Service* (MSCS), der im Lieferumfang von Microsoft® Windows 2003 in einer Aktiv/Passiv-Konfiguration enthalten ist. Installieren Sie GroupShield 7.0 auf demselben Laufwerk und in demselben Pfad auf allen Knoten des Clusters.

GroupShield 7.0 bietet keine Unterstützung für die Aktiv-Aktiv-Clusterkonfiguration. So implementieren Sie GroupShield in einer Aktiv-Aktiv-Konfiguration:

- GroupShield 7.0 muss auf beiden Knoten des Clusters installiert werden.
- Ändern Sie in der Services MMC den Starttyp des GroupShield Exchange-Dienstes in **Automatisch**.
- GroupShield sollte nicht mit dem Cluster-Administrator verwaltet werden. Der Ressourcentyp **McAfee Cluster Framework** sollte im Cluster-Administrator keiner Clustergruppe hinzugefügt werden.
- GroupShield 7.0 sollte auf den jeweiligen Clusterknoten nicht einzeln verwaltet werden.

Local Continuous Replication (LCR) unter Exchange Server 2007

Local Continuous Replication (LCR) ist eine Einzelserverlösung mit integrierter asynchroner Protokollierungstechnologie zum Erstellen und Verwalten einer Kopie einer Speichergruppe auf einer zweiten Datenträgergruppe, die mit dem gleichen Server wie die Produktionsspeichergruppe verbunden ist.

LCR ist keine Failover-Implementierung. GroupShield 7.0 kann daher ähnlich wie ein eigenständiger Postfachserver installiert und verwendet werden.

Clustered Continuous Replication (CCR) unter Exchange Server 2007

Die *Cluster Continuous Replication (CCR)* ist eine hochverfügbare Funktion von Microsoft® Exchange Server 2007. Sie kombiniert die in Microsoft® Exchange Server 2007 integrierte asynchrone Technologie zum Verteilen und Wiedergeben von Protokollen mit den Failover- und Verwaltungsfunktionen des Microsoft® Cluster-Dienstes.

Installieren Sie GroupShield 7.0 auf allen Knoten des Clusters gemäß der folgenden Installationsschritte.

Auf einem Exchange 2007 CCR-Cluster kann GroupShield für Exchange 7.0 nicht als Clusteranwendung installiert werden. Ein Ressourcentyp für GroupShield für Exchange 7.0 ist im **Cluster-Administrator** nicht verfügbar und kann dem virtuellen Exchange-Server nicht hinzugefügt werden. GroupShield für Exchange 7.0 muss auf allen Knoten des Clusters einzeln installiert und kann als eigenständige Instanz nicht eingesetzt werden.

Single Copy Cluster (SCC, N+1-Clusterkonfiguration) unter Exchange Server 2003 und 2007

A *Single Copy Cluster (SCC)* ist ein Cluster-Postfachserver, der freigegebenen Speicher in einer Failover-Clusterkonfiguration verwendet, damit mehrere Server eine einzelne Kopie der Speichergruppen verwalten können. Dieses Verfahren basiert auf den Failover- und Verwaltungsfunktionen des Microsoft® Cluster-Dienstes. Der Exchange Virtual Server verwendet eine eigene Netzwerkidentität und nicht die Identität eines im Cluster enthaltenen Knotens. Die Netzwerkidentität wird als Cluster-Postfachserver bezeichnet.

Sowohl der Exchange 2007-Postfachserver als auch der Exchange 2003-Server können in diesem Clustertyp bereitgestellt werden.

Installieren Sie GroupShield 7.0 auf allen Knoten des Clusters gemäß der folgenden Installationsschritte.

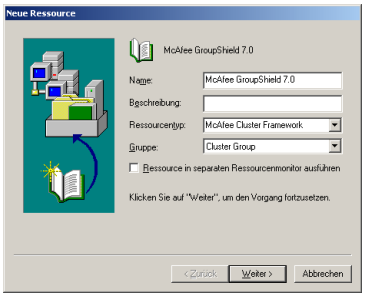
Nach der Installation der Knoten der Cluster sollte GroupShield für Exchange 7.0 den Clustergruppen hinzugefügt werden, in denen der virtuelle Exchange-Server enthalten ist.

Hinzufügen von GroupShield für Exchange als Ressource zu einer Clustergruppe

Wählen Sie unter **Cluster-Administrator** die Exchange-Clustergruppe aus, der die GroupShield für Exchange-Ressource hinzugefügt werden muss.

1 Wählen Sie im Menü **Datei** die Option **Neu** | **Ressource**. Der Assistent **Neue Ressource** wird angezeigt.

Abbildung 3-6 Neue Ressource



2 Geben Sie einen geeigneten **Namen** und eine **Beschreibung** für die **Ressource** ein.

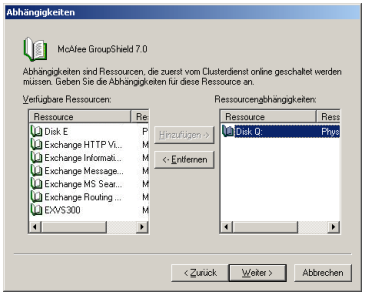
3 Wählen Sie in der Dropdown-Liste **Ressourcentyp** den Eintrag **McAfee Cluster Framework** aus.

4 Wählen Sie in der Dropdown-Liste **Gruppe** die **Clustergruppe** aus, zu der die GroupShield für Exchange-Ressource hinzugefügt werden muss.

5 Klicken Sie auf **Weiter**. Der Bildschirm **Mögliche Eigentümer** wird angezeigt. Stellen Sie sicher, dass die Knoten des Cluster, in dem GroupShield für Exchange installiert ist, in der Liste **Mögliche Eigentümer** enthalten ist.

6 Klicken Sie auf **Weiter**. Der Bildschirm **Abhängigkeiten** wird angezeigt. Stellen Sie eine Abhängigkeit zwischen dem aktuellen Ressourcentyp **McAfee Cluster Framework** zu dem Ressourcentyp **Physischer Datenträger** her.

Abbildung 3-7 Abhängigkeiten



7 Klicken Sie auf **Weiter**. Der Bildschirm **Parameter** wird angezeigt. Überprüfen Sie im Bereich **Freigegebenes Datenlaufwerk**, ob der Datenträger (im Bildschirm **Abhängigkeiten** ausgewählt) angezeigt wird.

8 Klicken Sie auf **Fertig stellen**. Ein Bestätigungsdialogfeld wird angezeigt.

9 Klicken Sie auf **OK**. Die Clusterressource wurde erfolgreich erstellt.

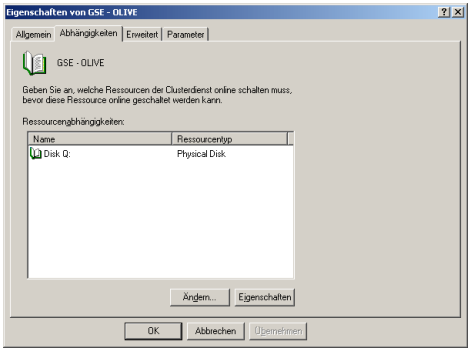
10 Klicken Sie unter **Cluster-Administrator** auf eine neu erstellte Ressource, und wählen Sie im Kontextmenü die Option **Online bringen** aus, um die GroupShield für Exchange 7.0-Ressource zu starten.

Wiederholen Sie die oben erläuterten Schritte für jede Exchange-Gruppe, der GroupShield für Exchange hinzugefügt werden soll.

Bei einer vorhandenen Ressource des Typs **McAfee Cluster FrameWork** wird die **Physikalischer Datenträger**-Ressourcenabhängigkeit zum Zeitpunkt der Erstellung hinzugefügt und darf auf der Registerkarte **Abhängigkeit** im Dialogfeld **Eigenschaften** der **<McAfee Cluster Framework** -Ressource**>** NICHT geändert werden.

Wenn die Abhängigkeit vom physikalischen Datenträger geändert werden muss, sollte die vorhandene Ressource des Typs **McAfee Cluster Framework** gelöscht und anschließend die Ressource mit der jeweiligen **Physikalischer Datenträger**-Abhängigkeit neu erstellt werden.

Abbildung 3-8 Cluster-Abhängigkeiten



Die Verwaltung (Bereitstellung, Konfiguration und Verteilung von Produktaktualisierungen) von GroupShield für Exchange 7.0 auf einem (n+1) Cluster wird von einem ePolicy Orchestrator-Server aus nicht unterstützt.

Eine Produktaktualisierung ist spezifisch für eine GroupShield für Exchange 7.0-Instanz auf einem virtuellen Exchange-Server. Bei einer Produktaktualisierung wird der Knoten, auf dem der virtuelle Exchange-Server mit GroupShield für Exchange 7.0 aktiv ist, aktualisiert. Bei einem Failover werden die Aktualisierungen von GroupShield für Exchange 7.0 automatisch auf einen anderen Knoten kopiert.

Deinstallation eines Clusters

1 Öffnen Sie den **Cluster-Administrator**.

2 Setzen Sie alle Ressourcen des Typs **McAfee Cluster Framework** in den Offline-Modus.

3 Löschen Sie alle Ressourcen des Typs **McAfee Cluster Framework**.

4 Schließen Sie den **Cluster-Administrator**.

Setzen Sie die Knoten des Clusters in den Passiv-Status, und deinstallieren Sie GroupShield für Exchange Version 7.0 wie unter *Deinstallieren von GroupShield für Exchange auf Seite 48* in diesem Handbuch erläutert. Wiederholen Sie diese Schritte für alle Knoten des Clusters.

Bei der Deinstallation der Software aus dem Cluster wird der McAfee-Ordner auf dem freigegebenen Laufwerk nicht gelöscht. Nach der Deinstallation der Software kann dieser Ordner manuell gelöscht werden.

Aktualisieren von GroupShield von v6.0.2 oder höher

Mit McAfee® GroupShield für Exchange Version 7.0 können Sie die Konfiguration einer früheren Produktversion aktualisieren. Bei der Aktualisierung auf eine neue Version von GroupShield für Exchange ist die Deinstallation der vorhandenen Version nicht erforderlich. Das Installationsprogramm aktualisiert die Installation auf die neue Version.

Die Aktualisierung von McAfee® SpamKiller Version 2.1.x wird nicht unterstützt. Deinstallieren Sie McAfee® SpamKiller mit der Funktion **Software**, bevor Sie die Installation von GroupShield für Exchange 7.0 starten.

Eine Aktualisierung der folgenden Produktversionen wird unterstützt:

- GroupShield für Exchange Version 6.0.2
- GroupShield für Exchange Version 6.0.2 + Patch1
- GroupShield für Exchange Version 6.0.3
- GroupShield für Exchange Version 6.0.3 + Patch1

Die Aktualisierung von GroupShield für Exchange Version 7.0 kann nur, wie bereits erwähnt, mit einer lizenzierten Version des Produkts ausgeführt werden.

1 Führen Sie den Setup-Wrapper von GroupShield für Exchange Version 7.0 auf GroupShield für Exchange Version 6.0.2 / 6.0.2+Patch1 / 6.0.3 / 6.0.3+Patch1 aus, um eine Aktualisierung auf GroupShield für Exchange Version 7.0 durchzuführen.

2 Wählen Sie die Add-Ons aus, die Sie installieren möchten.

3 Nach Abschluss der Installation ist Ihr System auf GroupShield für Exchange Version 7.0 aktualisiert.

Nach der Aktualisierung werden die Richtlinien, geplanten Tasks, Regeln und Konfigurationseinstellungen in GroupShield 7.0 übernommen.

4 Post-Installation und Wartung

Dieses Kapitel umfasst Informationen zu den Tätigkeiten im Anschluss an die Installation und zu Wartungsaufgaben:

- *Testen der GroupShield-Installation*
- *Isolieren mithilfe von McAfee Quarantine Manager*
- *Warten der GroupShield-Anwendung*
- *Deinstallieren der GroupShield für Exchange-Software*

Testen der GroupShield-Installation

Wenn Sie die Installation von GroupShield für Exchange abgeschlossen haben, sollten Sie die Installation testen. Damit wird sichergestellt, dass die Software korrekt installiert wurde und Viren und Spam in E-Mails erkannt werden.

Testen der Virenschutzkomponente

Zum Testen eines Antivirusprodukts wird empfohlen, eine EICAR-Virenschutztestdatei an eine E-Mail anzuhängen und die Nachricht über den Microsoft® Exchange Server 2003/2007 zu senden, auf dem gerade GroupShield für Exchange installiert wurde.

Die EICAR-Testdatei wurde gemeinsam von verschiedenen Herstellern von Antivirusprodukten entwickelt, um einen internationalen Standard zum Prüfen von Antivirusprodukten zu schaffen.

Diese Datei ist kein Virus. Löschen Sie die Datei, nachdem Sie Ihre Installation getestet haben, um zu vermeiden, dass arglose Benutzer alarmiert werden.

1 Kopieren Sie die folgende Zeile in eine eigene Datei, und speichern Sie diese unter dem Namen EICAR.COM.
`X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*`
Die Dateigröße beträgt 68 oder 70 Byte.

2 Senden Sie über den Exchange Server 2003/2007 eine E-Mail mit der EICAR-Testdatei als Anlage. Beim Überprüfen der E-Mail meldet GroupShield für Exchange unter Microsoft® Windows zwar, dass die EICAR-Testdatei erkannt wurde, kann diese Datei aber weder säubern noch reparieren, da es sich um eine Testdatei handelt.

3 GroupShield ersetzt die EICAR-Testdatei durch eine Warnmeldung.

Testen der Anti-Spam-Komponente

Sie können die Funktionstüchtigkeit der Software durch Ausführen des so genannten GTUBE-Tests (GTUBE = General Test Mail for Unsolicited Bulk Email) prüfen.
Die Test-E-Mail muss von einem externen E-Mail-Konto (einer anderen Domäne) gesendet werden.

Um diese Funktion testen zu können, muss die Add-On-Komponente McAfee Anti-Spam für GroupShield installiert sein.

1 Verfassen Sie eine neue E-Mail über ein externes Konto (Webmail).

2 Kopieren Sie die nachfolgende Zeichenfolge in den Nachrichtenteil der E-Mail.
`XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X`
Stellen Sie sicher, dass bei der Eingabe keine weiteren Leerzeichen oder Zeilenumbrüche hinzugefügt wurden.

3 Senden Sie diese E-Mail an eine E-Mail-Adresse auf dem Server, auf dem Sie das Anti-Spam-Add-On installiert haben. Anti-Spam für Exchange prüft die Nachricht, identifiziert sie als so genannte Junk-Mail und behandelt sie entsprechend.

Der GTUBE-Test hat Vorrang gegenüber schwarzen und weißen Listen. Weitere Informationen zur GTUBE-Testdatei finden Sie unter:

http://spamassassin.apache.org/

Testen der GroupShield-Installation mittels McAfee Virtual Technician

Führen Sie McAfee Virtual Technician aus, um die ordnungsgemäße Installation von GroupShield für Exchange zu testen. McAfee Virtual Technician sucht automatisch nach Abweichungen bzw. Änderungen, die seit der Installation des Produkts aufgetreten sind.

McAfee® Virtual Technician können Sie auf folgender Website herunterladen: *http://mvt.mcafee.com/mvt/index.asp*

Isolieren mithilfe von McAfee Quarantine Manager 4.1

McAfee® Quarantine Manager (MQM) kann als Repository zum Isolieren infizierter E-Mails verwendet werden. McAfee-Produkte (wie GroupShield für Exchange) verwenden eine vorher zugewiesene Portnummer für das Senden der Erkennungsinformationen an MQM.

McAfee® Quarantine Manager wiederum verwendet standardmäßig dieselbe Portnummer zum Freigeben oder Senden von Konfigurationsinformationen der erkannten E-Mail an das McAfee-Produkt. Die genannten Kommunikationsports in GroupShield und in der McAfee® Quarantine Manager-Benutzeroberfläche sollten gleich sein.

McAfee® Quarantine Manager kombiniert die Funktionalität für Quarantäne- und Anti-Spam-Verwaltung. Die Software bietet einen zentralen Ausgangspunkt für die Analyse und Behandlung isolierter E-Mails und Dateien. Elemente werden isoliert, da es sich um Spam oder Phishing handelt oder sie Viren, potenziell unerwünschte Programme oder anderen unerwünschten Inhalt enthalten. McAfee Quarantine Manager gestattet insbesondere die effektive Verwaltung unerwünschter E-Mails, die als Massensendungen verschickt werden, und Spam.

Dieses Handbuch enthält keine ausführlichen Informationen zum Installieren oder zum Einsatz von McAfee® Quarantine Manager. Weitere Informationen finden Sie im Produkthandbuch von McAfee Quarantine Manager v 4.1.

1. Installieren Sie GroupShield für Exchange auf <Server 1>.
2. Installieren Sie McAfee Quarantine Manager Version 4.1 auf <Server 2>.
3. Starten Sie die GroupShield für Exchange-Benutzeroberfläche über <Server 1>.
4. Klicken Sie auf **Einstellungen & Diagnose** | **Erkannte Elemente**.

5 Wählen Sie unter **McAfee Quarantine Manager** die Option **Aktiviert** aus.

6 Geben Sie die **IP-Adresse** des Servers <Server 2> ein, auf dem McAfee Quarantine Manager installiert wurde.

7 Verwenden Sie die Standardwerte für **Port** und **Rückrufport**, oder ändern Sie diese gemäß der McAfee Quarantine Manager-Serverkonfiguration.

8 Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern.

Anschließend startet GroupShield die Isolierung erkannter Elemente auf dem McAfee Quarantine Manager-Server. Sie werden außerdem in der lokalen Datenbank protokolliert.

Auf dem McAfee Quarantine Manager-Server müssen McAfee Quarantine Manager Version 4.1 Patch1 und HotFix 285970 installiert werden. Nach Installation dieser Patch- und HotFix-Versionen können Sie isolierte Elemente auf dem Server freigeben.

Isolierte Elemente, die als Viren identifiziert wurden, können nicht freigegeben werden.

Zum Deaktivieren der Isolierung auf McAfee Quarantine Manager wählen Sie **Einstellungen & Diagnose** | **Erkannte Elemente**, und deaktivieren Sie **Aktiviert**. Klicken Sie anschließend auf **Übernehmen**. So führt GroupShield weiterhin die Isolierung auf der lokalen Datenbank durch.

Aktualisieren von schwarzen und weiße Listen

Mit dem Befehlszeilentool zum Aktivieren schwarzer und weißer Listen können Sie die schwarzen und weißen Benutzerlisten in GroupShield Version 6.0.x auf 7.0 aktualisieren. Bei den Befehlszeilenparametern spielt die Groß-/Kleinschreibung keine Rolle, außerdem können Sie bei Verwendung des Aktualisierungstools UNC-Pfade verwenden.

1 Melden Sie sich mit einem Administratorkonto bei dem Computer an, auf dem sich die schwarzen und weißen Benutzerlisten von GroupShield für Exchange Version 6.0.x befinden.

2 Erstellen Sie ein temporäres Verzeichnis auf der lokalen Festplatte.

3 Laden Sie das **UserBWListUpgrade.ZIP**-Archiv herunter, und extrahieren Sie die Dateien in das temporäre Verzeichnis.

4 Führen Sie an der Eingabeaufforderung folgenden Befehl aus:

```
bwl -m <Quellpfad> <Zielpfad> [-d] [value]
```

Parameter:

-m: Aktualisiert schwarze und weiße Benutzerlisten.

<Quellpfad>: Gibt den Verzeichnispfad der vorhandenen schwarzen und weißen Benutzerlisten von GroupShield 6.x an.

<Zielpfad>: Gibt den Verzeichnispfad an, in dem die generierte BWLIST.XML-Datei gespeichert werden soll. Die generierte Ausgabe-XML-Datei kann mit dem Tool für Import/Export in die McAfee Quarantine Manager-Datenbank importiert werden.

-d: Ermöglicht das Beheben von Fehlern. Die Fehlersuchprotokolldatei DEBUG.TXT wird im aktuellen Verzeichnis erstellt.

[value]: „1" ermöglicht das Beheben von Fehlern. Jeder andere an diesen Parameter übergebene Wert deaktiviert die Fehlerbehebung und ist FALSE. Der Standardwert ist auf FALSE gesetzt.

-h: Hilfe

Die Parameter können auch wie folgt ersetzt werden:

- m durch **/m**

-d durch **/d**

-h durch **/h**

Syntax-Beispiele:

- So aktualisieren Sie schwarze und weiße Benutzerlisten von GroupShield 6.x auf Version 7.0

```
bwl -m "c:\GSE_60_BWL_Path\" "c:\GSE_70_BWL_Path"
```

- So aktualisieren Sie schwarze und weiße Benutzerlisten von GroupShield 6.x auf Version 7.0 mit Fehlersuchprotokollen

```
bwl -m "c:\GSE_60_BWL_Path\" "c:\GSE_70_BWL_Path" -d 1
```

- So aktualisieren Sie mithilfe eines UNC-Pfads schwarze und weiße Benutzerlisten von GroupShield 6.x auf Version 7.0 mit Fehlersuchprotokollen

```
bwl -m "c:"\\server-name\shared-resource-pathname\"
"c:\GSE_70_BWL_Path" -d 1
```

Warten der GroupShield-Anwendung

Die GroupShield für Exchange-Software verfügt über Tools zur Wartung der Installation. Einzelheiten hierzu finden Sie in den folgenden Abschnitten:

- *Ändern der GroupShield-Installation*
- *Reparieren der GroupShield-Installation*
- *Wiederherstellen der Standardkonfiguration*

Ändern der GroupShield-Installation

Um die installierten Programmfunktionen von GroupShield für Exchange zu ändern, führen Sie das Setup-Programm von **McAfee GroupShield für Exchange** aus, oder verwenden Sie die Windows-Funktion **Software**.

Ändern von GroupShield

1. Melden Sie sich mit einem Administratorkonto bei dem Computer an, auf dem Microsoft® Exchange Server 2003/2007 installiert ist.
2. Stellen Sie sicher, dass Server und Clients heruntergefahren sind.
3. Im Menü **Start** wählen Sie **Einstellungen** und anschließend **Systemsteuerung**. Das Fenster **Systemsteuerung** wird angezeigt.
4. Doppelklicken Sie auf die Option **Software**. Das Dialogfeld **Software** wird angezeigt.
5. Wählen Sie in der Liste **McAfee GroupShield für Exchange**.
6. Klicken Sie auf **Ändern/Entfernen**. Das Feld **Anwendungswartung** wird angezeigt.
7. Wählen Sie **Ändern** aus, und klicken Sie auf **Weiter**.
8. Nehmen Sie im Funktionsdialogfeld von **McAfee GroupShield für Exchange** die gewünschten Funktionsänderungen vor, und klicken Sie anschließend auf **Weiter**. Nachdem die Installation aktualisiert wurde, wird eine Bestätigungsmeldung angezeigt.
9. Klicken Sie auf **Fertig stellen**, um das Dialogfeld zu schließen.

Reparieren der GroupShield-Installation

Um GroupShield für Exchange zu reparieren, sollten Sie die Windows-Funktion **Software** verwenden oder das Setup-Programm von GroupShield für Exchange ausführen.

Wenn festgestellt wird, dass GroupShield-Dateien beschädigt oder gelöscht wurden, werden Sie durch die entsprechenden Dateien ersetzt. Die Konfiguration bleibt dabei unverändert, und es werden keine Einstellungen geändert.

Reparieren von GroupShield

1. Melden Sie sich mit einem Administratorkonto bei dem Computer an, auf dem Microsoft® Exchange Server 2003/2007 installiert ist.
2. Stellen Sie sicher, dass Server und Clients heruntergefahren sind.
3. Im Menü **Start** wählen Sie **Einstellungen** und anschließend **Systemsteuerung**. Das Fenster **Systemsteuerung** wird angezeigt.
4. Doppelklicken Sie auf die Option **Software**. Das Dialogfeld **Software** wird angezeigt.
5. Wählen Sie in der Liste **McAfee GroupShield für Exchange**.
6. Klicken Sie auf **Ändern/Entfernen**. Das Feld **Anwendungswartung** wird angezeigt.
7. Wählen Sie **Reparieren** aus, und klicken Sie auf **Weiter**.
   Das Funktionsdialogfeld von **McAfee GroupShield for Exchange** wird angezeigt. Nachdem die Installation aktualisiert wurde, wird eine Bestätigungsmeldung angezeigt.
8. Klicken Sie auf **Fertig stellen**, um das Dialogfeld zu schließen.

Wiederherstellen der Standardkonfiguration

Zum Wiederherstellen der Standardeinstellungen und -werte über die Benutzeroberfläche klicken Sie auf **Einstellungen & Diagnose** | **Import- und Exportkonfiguration** | **Standard wiederherstellen**.

Alternativ können Sie die Standardeinstellungen und -werte manuell wiederherstellen, indem Sie folgende Schritte ausführen:

1. Stoppen Sie alle Exchange-Server, und beenden Sie die GroupShield für Exchange-Dienste auf dem Host-Computer.
2. Ersetzen Sie die Datei **McAfeeConfig.XML** durch die Kopie **<Installationsverzeichnis>\Config\Default\McAfeeConfig.XML**
3. Ersetzen Sie die Datei CS_RULES_EN.XML durch die Kopie **<Installationsverzeichnis>\Config\Default\<0409>\CS_RULES_EN.XML <für Englisch>**
4. Starten Sie die GroupShield für Exchange-Dienste auf dem Host-Computer.
5. Starten Sie die Exchange-Server auf dem Host-Computer.

Deinstallieren von GroupShield für Exchange

Um GroupShield für Exchange zu entfernen, sollten Sie die Windows-Funktion **Software** verwenden oder das Setup-Programm von GroupShield für Exchange ausführen.

Entfernen von GroupShield für Exchange

1. Melden Sie sich mit einem Administratorkonto bei dem Computer an, auf dem Microsoft® Exchange Server 2003/2007 installiert ist.
2. Stellen Sie sicher, dass die GroupShield für Exchange-Dienste auf Server und Client beendet wurden.
3. Im Menü **Start** wählen Sie **Einstellungen** und anschließend **Systemsteuerung**. Das Fenster **Systemsteuerung** wird angezeigt.
4. Doppelklicken Sie auf die Option **Software**. Das Dialogfeld **Software** wird angezeigt.
5. Wählen Sie in der Liste **McAfee GroupShield für Exchange**.
6. Klicken Sie auf **Ändern/Entfernen**. Das Feld **Anwendungswartung** wird angezeigt.
7. Wählen Sie **Entfernen** aus, und klicken Sie auf **Weiter**.
8. Das Dialogfeld **McAfee GroupShield für Exchange Deinstallation** wird angezeigt. Klicken Sie auf **Weiter**.
9. Nachdem die Software entfernt wurde, wird eine Bestätigungsmeldung angezeigt. Klicken Sie auf **Fertig stellen**, um das Dialogfeld zu schließen.

5 Integrieren in ePolicy Orchestrator 3.6

Einführung

In diesem Kapitel wird die Konfiguration von GroupShield für Exchange mithilfe der Verwaltungssoftware McAfee ePolicy Orchestrator Version 3.6 erläutert. Damit Sie dieses Handbuch richtig einsetzen können, sollten Sie mit den Funktionen von ePolicy Orchestrator vertraut sein. Weitere Informationen hierzu finden Sie im *ePolicy Orchestrator v3.6-Produkthandbuch*.

ePolicy Orchestrator stellt die gemeinsame Steuerungszentrale für alle im Unternehmen eingesetzten McAfee-Antivirusprodukte dar, in der Sie Antivirusrichtlinien verwalten und Berichte zu Antiviruseignissen und Virusaktivitäten einsehen können. Mit ePolicy Orchestrator können Sie GroupShield für Exchange auf allen Zielcomputern im Netzwerk konfigurieren; die individuelle Konfiguration der Computer erübrigt sich.

In diesem Kapitel werden folgende Themen behandelt:

- Einchecken des ePolicy Orchestrator-Agenten in das ePolicy Orchestrator-Repository
- Einchecken von GroupShield für Exchange-Paket und -NAP-Dateien in das ePolicy Orchestrator-Repository
- Konfigurieren der ePolicy Orchestrator-Agentenfunktionen
- Einrichten und Durchsetzen von Antivirusrichtlinien auf den Zielsystemen

Dieses Handbuch enthält keine ausführlichen Informationen zum Installieren oder zum Einsatz von ePolicy Orchestrator. Weitere Informationen hierzu finden Sie im *ePolicy Orchestrator v3.6-Produkthandbuch*.

Voraussetzungen für die Verwendung von ePolicy Orchestrator 3.6

Bevor Sie GroupShield für Exchange mit ePolicy Orchestrator verwalten können müssen Sie den ePolicy Orchestrator-Agenten auf dem Computer installieren.

Einführung in die ePolicy Orchestrator-Konsole

Die Benutzerschnittstelle für den Zugriff auf ePolicy Orchestrator basiert auf *Microsoft® Management Console* (MMC). Über die MMC-Schnittstelle registrieren und konfigurieren Sie die verschiedenen Produkte von GroupShield für Exchange, die mit ePolicy Orchestrator verwaltet werden können. Die Konsole verwendet MMC-Standardfunktionen.

Die Konsole besteht aus zwei Bereichen. Wenn Sie sich zum ersten Mal am Server anmelden, wird das Konsolenstammverzeichnis im linken Bereich der Konsole hervorgehoben angezeigt.

- Die Konsolenstruktur ist der Navigationsbereich der Konsole. Darin werden die Server, Workstation und Anwendungen angezeigt, die Sie mithilfe von ePolicy Orchestrator verwalten können.
- Im rechten Bereich der Konsole befindet sich der Detailbereich. Je nach ausgewähltem Element in der Konsolenstruktur kann der Detailbereich in einen oberen und einen unteren Detailbereich unterteilt sein.

Der Aufbau der Konsole ändert sich entsprechend den markierten Objekten in der Konsolenstruktur bzw. des Detailbereichs.

Der Agent ist eine dezentrale Komponente von ePolicy Orchestrator, die auf jedem System im Netzwerk installiert sein muss. Der Agent sammelt und sendet Daten zwischen ePolicy Orchestrator-Server und Repositorys und verwaltet netzwerkweit Installationen von GroupShield für Exchange. Über die Konfiguration des Agenten und die Richtlinieneinstellungen bestimmen Sie, inwieweit der Agent die Kommunikation und Aktualisierungen in Ihrer Umgebung unterstützt.

Annahme:

- Computer 1: ePolicy Orchestrator Version 3.6 ist auf einem unterstützten Betriebssystem installiert und konfiguriert.
- Computer 2: Microsoft® Exchange Server 2003/2007 ist auf dem Server installiert und konfiguriert.
- Der Exchange-Server wird in die Liste der verwalteten Server von ePolicy Orchestrator in die Verzeichnisebene aufgenommen.
- Der auf dem ePolicy Orchestrator-Server installierte McAfee Common Agent in der Version 3.6.0.444 sollte auf Version 3.6.0.453 oder höher aktualisiert werden.
- Über die ePolicy Orchestrator-Serverkonsole wird der ePolicy Orchestrator-Agent installiert oder auf den Exchange-Server verschoben.

Bevor Sie beginnen

1. Erstellen Sie ein temporäres Verzeichnis im Netzwerk oder auf dem lokalen Laufwerk.
2. Für die Installation führen Sie einen der folgenden Schritte aus, abhängig davon, wie Sie die Software erhalten haben:
   - Legen Sie die CD-ROM in das Laufwerk des Computers ein, und kopieren Sie die Installationsdateien in das erstellte temporäre Verzeichnis.
   - Laden Sie das NAP-/ZIP-Archiv herunter, und extrahieren Sie die Dateien in das temporäre Verzeichnis.

Die Anti-Spam- und Anti-Phishing-Funktionalität ist nur verfügbar, wenn Sie nach der Installation die Komponente McAfee Anti-Spam für GroupShield ausgewählt haben. Um die Anti-Spam- und Anti-Phishing-Funktionalität zu installieren, müssen Sie das erforderliche Paket in das Repository einchecken und dann implementieren. Wenn das Evaluierungspaket ausgebracht worden ist und Sie auf die lizenzierte Version hochstufen möchten, müssen Sie das Lizenzpaket einchecken und ausbringen.

Installation

1 Melden Sie sich mit einem Administratorkonto beim ePolicy Orchestrator-Server an. Die **ePolicy Orchestrator-Konsole** wird angezeigt.

Erstellen eines neuen Standorts

2 Klicken Sie mit der rechten Maustaste auf **Verzeichnis** | **Neu** | **Standort**. Daraufhin wird das Dialogfeld **Standorte hinzufügen** angezeigt.

3 Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neuer Standort** wird angezeigt.

Sie können einen neuen Standort erstellen, um eine bestimmte Gruppe von Computern zu verwalten.

4 Benennen Sie im Feld **Name** den neuen Standort. Wenn es sich bei dem neuen Standort um eine Domäne handelt und Sie alle Computer in der Domäne einbeziehen möchten, aktivieren Sie die Kontrollkästchen **Domäne** und **Computer als untergeord. Knoten einbeziehen**.

5 Klicken Sie auf **OK**, um den neuen Standort hinzuzufügen. Daraufhin wird das Dialogfeld **Standorte hinzufügen** angezeigt.

6 Deaktivieren Sie das Kontrollkästchen **Agentenpaket senden**, und klicken Sie auf **OK**, um den neuen Standort **<Standortname>** in den linken Bereich zu übernehmen.

Hinzufügen eines Computers in die Liste

7 Klicken Sie mit der rechten Maustaste auf **Verzeichnis** | **<Standortname>** | **<Neu>** | **Computer**. Daraufhin wird das Dialogfeld **Computer hinzufügen** angezeigt.

8 Klicken Sie auf **Durchsuchen**, wählen Sie einen Computer aus dem Netzwerk aus, und bestätigen Sie durch Klicken auf **OK**. Daraufhin wird das Dialogfeld **Computer hinzufügen** angezeigt.

9 Wählen Sie **Agentenpaket senden**, geben Sie die erforderlichen **Anmeldeinformationen für Push-Installation des Agenten** ein, und klicken Sie zum Senden des Agenten an den neu hinzugefügten Computer auf **OK**.

Falls Sie das Kontrollkästchen **Agenteninstallations-GUI unterdrücken** deaktiviert haben, wird während der Installation nicht die Benutzeroberfläche für die Agenteninstallation auf dem Client-Computer angezeigt.

So aktivieren Sie das Taskleistensymbol für den ePolicy Orchestrator-Agenten auf dem Client-Computer

a Klicken Sie im rechten Bereich auf **ePO-Agent**.

b Klicken Sie für den ePolicy Orchestrator-Agenten auf **McAfee-Standard**. Die Seite **ePolicy Orchestrator-Agent** wird geöffnet.

c Wählen Sie **Agenten-Taskleistensymbol anzeigen** aus.

d Klicken Sie auf **Alles übernehmen**.

Senden einer Agentenreaktivierung

10 Klicken Sie in der ePolicy Orchestrator-Konsole mit der rechten Maustaste auf den **Standort** oder Exchange-Server, auf dem GroupShield für Exchange installiert werden soll.

11 Klicken Sie auf **Agentenreaktivierung**. Das Fenster **Agentenreaktivierung** wird angezeigt.

12 Stellen Sie im Dialogfeld **Agentenreaktivierung** für die Option **Agenten-Zufallsgenerator** den Wert **0** (Minuten) ein.

13 Aktivieren Sie das Kontrollkästchen **Alle Produkteigenschaften erhalten**, und klicken Sie auf **OK**, um die Installation abzuschließen.

Hinzufügen von GroupShield-Installationspaketdateien zum ePolicy-Repository

14 Klicken Sie auf **Repository**. Die Seite **Repository** wird geöffnet.

15 Klicken Sie auf **Paket einchecken**. Der Assistent für das Einchecken von Paketen wird geöffnet.

16 Klicken Sie auf **Weiter**. Der Assistent zum Auswählen des Pakettyps wird angezeigt.

17 Wählen Sie **Produkte oder Aktualisierungen**, und klicken Sie anschließend auf **Weiter**. Das Dialogfeld **Paket einchecken - Browse** wird angezeigt.

18 Klicken Sie auf **Durchsuchen**, und wechseln Sie in den temporären Ordner, in dem Sie das Installationspaket entpackt haben.

19 Wählen Sie die Datei **PkgCatalog.z** aus, klicken Sie auf **Öffnen** und dann auf **Weiter**. Der Assistent zum Einchecken von Paketen zeigt die **Produktbezeichnung**, die **Version**, den **Pakettyp** und die **Sprache** an.

20 Klicken Sie auf **Fertig stellen**, um die Paketdatei einzuchecken.

21 Nach Abschluss des Eincheckvorgangs klicken Sie auf **Schließen**.

Hinzufügen der NAP-Datei für die GroupShield-Software zum Repository

1. Klicken Sie auf **Repository**. Die Seite **Repository** wird geöffnet.
2. Klicken Sie auf **NAP einchecken**. Der Assistent für die Konfiguration des Software-Repository wird angezeigt.
3. Wählen Sie **Neue zu verwaltende Software hinzufügen**, und klicken Sie auf **Weiter**. Das Dialogfeld **Software-Paket wählen** wird angezeigt.
4. Wählen Sie die Produkt-NAP-Datei aus dem temporären Ordner aus, und klicken Sie auf **Öffnen**.
   Die NAP-Datei wird extrahiert und in das ePolicy Orchestrator-Repository kopiert. Sobald der Vorgang ordnungsgemäß abgeschlossen ist, wird ein Dialogfeld mit einer entsprechenden Meldung angezeigt.
5. Klicken Sie auf **OK**.

Hinzufügen der NAP-Datei für GroupShield-Berichte zum Repository

1. Klicken Sie auf **Repository**. Die Seite **Repository** wird geöffnet.
2. Klicken Sie auf **NAP einchecken**. Der Assistent für die Konfiguration des Software-Repository wird angezeigt.
3. Wählen Sie **Neue Berichte hinzufügen**, und klicken Sie auf **Weiter**. Das Dialogfeld **Software-Paket wählen** wird angezeigt.
4. Wählen Sie die Berichts-NAP-Datei aus dem temporären Ordner aus, und klicken Sie auf **Öffnen**.
   Die Berichts-NAP-Datei wird extrahiert und in das ePolicy Orchestrator-Repository kopiert. Sobald der Vorgang ordnungsgemäß abgeschlossen ist, wird ein Dialogfeld mit einer entsprechenden Meldung angezeigt.
5. Klicken Sie auf **OK**.

Installieren von GroupShield auf dem Client-Computer

1 Wählen Sie in der ePolicy Orchestrator-Konsole den **Standort** oder den Exchange-Server für die GroupShield.Installation aus, und klicken Sie auf die Registerkarte **Tasks**. Die Seite mit dem Ausbringungs-Task wird angezeigt.

2 Doppelklicken Sie auf den Task **Ausbringung**. Daraufhin wird das Dialogfeld **ePolicy Orchestrator-Planer** angezeigt.

3 Deaktivieren Sie auf der Registerkarte **Tasks** das Kontrollkästchen **Vererben**, und wählen Sie die Option **Aktivieren (geplanter Task wird zu festgelegter Zeit ausgeführt)** aus.

4 Klicken Sie auf der Registerkarte **Tasks** auf **Einstellungen**. Die Seite **Taskeinstellungen** wird angezeigt.

5 Deaktivieren Sie das Kontrollkästchen **Vererben**. Wählen Sie in der Produktliste für den Eintrag **GroupShield für Exchange** die Aktion **Installieren** aus.

6 Deaktivieren Sie das Kontrollkästchen **Diesen Task bei jedem Richtlinienumsetzungsintervall ausführen**.

7 Klicken Sie auf **OK**.

8 Klicken Sie auf die Registerkarte **Zeitplan**. Deaktivieren Sie das Kontrollkästchen **Vererben**.

9 Wählen Sie bei **Task planen** die Option **Sofort ausführen** aus, und klicken Sie auf **Übernehmen**.

10 Klicken Sie auf **OK**, um die Planung des Ausbringungs-Tasks abzuschließen.

11 Senden Sie eine Agentenreaktivierung.

Weitere Informationen zum Senden einer Agentenreaktivierung finden Sie unter *Senden einer Agentenreaktivierung auf Seite 53*.

Aktualisieren von GroupShield für Exchange Version 6.0.x-NAP-Einstellungen

Annahme:

- ePolicy Orchestrator Version 3.6 ist auf dem Server installiert.
- NAP-Dateien für GroupShield für Exchange Version 6.0.2 oder Version 6.0.3 sind eingecheckt.
- NAP-Datei für GroupShield für Exchange Version 7.0 ist eingecheckt.
- Es wurde keine neue Richtlinie in den NAP-Einstellungen von GroupShield für Exchange Version 7.0 erstellt.

Importieren von GroupShield für Exchange Version 6.x-NAP-Einstellungen

1 Melden Sie sich mit einem Administratorkonto beim ePolicy Orchestrator-Server an.

2 Erstellen Sie ein temporäres Verzeichnis im Netzwerk oder auf dem lokalen Laufwerk.

3 Für die Installation führen Sie einen der folgenden Schritte aus, abhängig davon, wie Sie die Software erhalten haben:

- Legen Sie die CD-ROM in das Laufwerk des Computers ein, und kopieren Sie die Installationsdateien in das erstellte temporäre Verzeichnis.
- Laden Sie das Archiv **ePOGSENPUpgrade.ZIP** herunter, und extrahieren Sie die Datei in das temporäre Verzeichnis.

4 Wechseln Sie im Windows Explorer zu dem Ordner, in den Sie die Installationsdateien kopiert haben, und doppelklicken Sie auf **EPOGSEUPGRADE.EXE**.

Dieses Tool exportiert nur die in der NAP-Datei von GroupShield für Exchange Version 6.0.2 oder Version 6.0.3 gespeicherten Konfigurationen in die GroupShield für Exchange 7.0-NAP-Datei. Sie können weiterhin alle GroupShield-Versionen (6.0.x und 7.0) über den ePolicy Orchestrator-Server verwalten.

5 Bei erfolgreicher Aktualisierung wird folgende Meldung angezeigt: **EPO-Aktualisierung von GSE6.0 auf GSE7.0 erfolgreich abgeschlossen...**. Wenn die Aktualisierung fehlgeschlagen ist, führen Sie die Anweisungen auf dem Bildschirm aus.

Fehler oder Ausnahmen während der Aktualisierung werden in der Datei **EPODEBUGTRACE.TXT** protokolliert.

Konfigurieren von GroupShield-Richtlinien

In diesem Abschnitt erfahren Sie mehr über die Durchsetzung von Richtlinien mithilfe von ePolicy Orchestrator. Es gibt zwei wichtige Schritte:

1. In ePolicy Orchestrator können Sie die Namen der Zielcomputer oder den Standort im Netzwerk sowie die Richtlinien auswählen, die auf diese Computer angewendet werden sollen.
2. Mithilfe des ePolicy Orchestrator-Agenten können Sie alle Richtlinien auf dem Exchange-Server durchsetzen. Jeder Computer befolgt dann die neue Richtlinie. Bisherige mit GroupShield für Exchange konfigurierte Richtlinien werden ignoriert.

Verwalten von Richtlinien

Mithilfe der ePolicy Orchestrator-Konsole können Sie Richtlinien für Gruppen von Computern oder einen einzelnen Computer verwalten. Diese Richtlinien setzen die Konfigurationseinstellungen der einzelnen Computer außer Kraft. Informationen bezüglich Richtlinien und ihrer Durchsetzung finden Sie im *ePolicy Orchestrator-Produkthandbuch*.

Wählen Sie vor dem Konfigurieren von Richtlinien die Gruppe der Computer aus, deren GroupShield-Richtlinien Sie bearbeiten möchten. Sie können GroupShield-Richtlinien mithilfe der Seiten und Registerkarten bearbeiten, die im Detailbereich der ePolicy Orchestrator-Konsole zur Verfügung stehen. Diese Seiten sind identisch mit jenen, auf die Sie direkt über die Benutzeroberfläche von GroupShield zugreifen können.

Nachdem Sie die entsprechenden Richtlinien geändert und die Änderungen für den gewünschten Computer bzw. die Gruppe von Computern gespeichert haben, können Sie die neuen Einstellungen über den ePolicy Orchestrator-Agenten ausbringen.

Ändern von Richtlinien für GroupShield mithilfe von ePolicy Orchestrator

1. Melden Sie sich mit einem Administratorkonto beim ePolicy Orchestrator-Server an.
2. Wählen Sie in der Konsolenstruktur unter **ePolicy Orchestrator** | **<SERVER>** | **Verzeichnis** den Standort, die Gruppe, den einzelnen Computer oder das gesamte Verzeichnis aus, auf welchen/s diese Richtlinien angewendet werden sollen.
3. Im Detailbereich werden die Registerkarten **Richtlinien**, **Eigenschaften** und **Tasks** angezeigt.
4. Klicken Sie auf der Registerkarte **Richtlinien** unter **GroupShield für Exchange** für eine **Kategorie** auf **McAfee-Standard**, um die standardmäßigen Richtlinieneinstellungen anzuzeigen. Das Dialogfeld **Richtlinieneinstellungen** wird angezeigt.

5 Klicken Sie auf **Kopie erstellen**, um eine Kopie der Richtlinieneinstellungen zu erstellen oder zu speichern. Das Dialogfeld **Richtlinie kopieren** wird geöffnet.

6 Wählen Sie **Aktuelle Richtlinie kopieren** oder **Erstellen einer Richtlinie mit Vererbung für alle Registerkarten** aus.

7 Geben Sie unter **Neuer Richtlinienname** einen Namen ein.

8 Aktivieren oder deaktivieren Sie **Diese neue Richtlinie dem aktuellen Knoten zuweisen (unterbricht Vererbung)**, und klicken Sie dann auf **OK**.

Erstellen einer neuen Richtlinie für eine Kategorie

1 Klicken Sie im Detailbereich von ePolicy Orchestrator unter **GroupShield für Exchange** für eine **Kategorie** auf **Bearbeiten**.

2 Klicken Sie auf die Dropdown-Liste **Richtlinienname**, und wählen Sie **Neue Richtlinie** aus. Das Dialogfeld **Neue Richtlinie erstellen** wird angezeigt.

Sie können die **McAfee-Standard**-Richtlinieneinstellungen nicht für eine ausgewählte **Kategorie** konfigurieren. Um eine ausgewählte Kategorie zu konfigurieren, müssen Sie eine neue Richtlinie oder eine Richtlinienkopie für die ausgewählte **Kategorie** erstellen.

Tabelle 5-1 Richtlinienoptionen

Neuer Richtlinienname	Geben Sie den neuen Richtliniennamen für die Kategorie ein, die Sie erstellen möchten.
Folgende Richtlinie verdoppeln	Erstellt eine Kopie der Richtlinie für die ausgewählte Kategorie. Wählen Sie die Richtlinie aus der Dropdown-Liste aus.
Erstellen einer Richtlinie mit Vererbung für alle Registerkarten	Erstellt eine neue Richtlinie, in der die Einstellungen aller Registerkarten vererbt werden.

3 Konfigurieren Sie die erforderlichen Optionen der ursprünglichen Richtlinie, und klicken Sie dann auf **OK**, um die neue Richtlinie zu erstellen.

4 Klicken Sie auf **Übernehmen**, um diese Einstellungen zu speichern.

Bearbeiten einer vorhandenen Richtlinie (Nicht Standard)

1 Klicken Sie im Detailbereich von **ePolicy Orchestrator** unter **GroupShield für Exchange** für eine **Kategorie** auf **Bearbeiten**.

2 Konfigurieren Sie die erforderlichen Optionen, und klicken Sie anschließend auf **Übernehmen**, um die Richtlinie zu speichern.

Wenn Sie eine Richtlinie nicht mehr durchsetzen möchten, klicken Sie in ePolicy Orchestrator im Eintrag **GroupShield für Exchange** für **Richtlinien durchsetzen** auf **Bearbeiten**, und wählen Sie aus der Dropdown-Liste **Richtlinienname** die Option **(Nein)** aus.

Planen von Tasks

Zum Erkennen von Viren, Spam und Phishing verwendet GroupShield beim Scannen die Regel- und Virusdefinitionsdateien (DATs). Täglich werden viele neue Viren erkannt, und McAfee erstellt ständig neue DAT-Dateien, um Schutz vor diesen Viren zu gewähren. Für einen bestmöglichen Schutz können Sie mithilfe von ePolicy Orchestrator festlegen, von wo die neuesten Aktualisierungsdateien abgerufen werden sollen, und Zeitpläne für die Ersetzung veralteter DAT- und Regeldateien und für Scans auf Anforderung erstellen.

Mit ePolicy Orchestrator 3.6 können Sie folgende geplante Tasks für GroupShield für Exchange erstellen:

- AutoUpdate
- Scannen auf Anforderung

Geplante Tasks für einen Computer lassen sich auf Grundlage der Ortszeit oder der GMT (Greenwich Mean Time) ausführen. ePolicy Orchestrator kann jedoch den Fortschritt des geplanten Tasks nicht überwachen. Deshalb sollten Sie in regelmäßigen Abständen die Protokolldatei auf dem Server daraufhin prüfen, ob der geplante Task erfolgreich durchgeführt wurde.

AutoUpdate-Task

GroupShield 7.0 kann einen vollen Schutz nur dann bieten, wenn Sie die Virusdefinitionsdatei (DAT-Datei), die Anti-Spam-Regeln, das Anti-Spam-Modul und das Virenscanmodul regelmäßig aktualisieren. Es wird empfohlen, die DAT-Dateien täglich zu aktualisieren und regelmäßig die McAfee AVERT-Website (AVERT = Anti-Virus Emergency Response Team) auf neue DAT-Dateien zu überprüfen. Wenn Sie über mehrere Server in der aktuellen Domäne verfügen, können Sie einen dieser Server zum Herunterladen der neuesten DAT-Datei und des neuesten Scanmoduls verwenden und die übrigen zum Übernehmen der Dateien von diesem Server konfigurieren. Die Server können unabhängig von den verwendeten Betriebssystemen Dateien für mehrere Betriebssysteme herunterladen.

Erstellen eines AutoUpdate-Tasks

1 Melden Sie sich mit einem Administratorkonto beim ePolicy Orchestrator-Server an.

2 Klicken Sie in der Konsolenstruktur unter **ePolicy Orchestrator** mit der rechten Maustaste auf **Verzeichnis** oder den gewünschten Standort, die Gruppe bzw. den Computer, und wählen Sie die Option **Task planen** aus.
Alternativ können Sie auch im oberen Detailbereich auf die Registerkarte **Tasks** klicken. Klicken Sie dann mit der rechten Maustaste auf den Bereich, und wählen Sie **Task planen** Das Dialogfeld **Task planen** wird geöffnet.

3 Geben Sie den Namen des neuen Tasks ein.

4 Wählen Sie in der Dropdown-Liste **Task-Typ** die Option **GroupShield für Exchange 7.0 AutoUpdate-Task** aus.

5 Klicken Sie auf **OK**. Der erstellte Task wird auf der Registerkarte **Tasks** aufgelistet.

6 Senden Sie eine Agentenreaktivierung.

Weitere Informationen zum Senden einer Agentenreaktivierung finden Sie unter *Senden einer Agentenreaktivierung auf Seite 53*.

Konfigurieren eines AutoUpdate-Tasks

Nachdem Sie einen neuen AutoUpdate-Task erstellt haben, können Sie den Task auf die spezifischen Anforderungen anpassen.

1 Klicken Sie im oberen Detailbereich auf der Registerkarte **Tasks** mit der rechten Maustaste auf den Task, und wählen Sie dann **Task bearbeiten**. Daraufhin wird das Dialogfeld **ePolicy Orchestrator-Planer** angezeigt.

2 Klicken Sie dort auf **Einstellungen**, und bearbeiten Sie die erforderlichen Optionen auf den Registerkarten **Task** und **Zeitplan**. Die Seite **Aktualisierungstask** wird mit der Nachricht **Für diesen Task sind keine weiteren Einstellungen erforderlich** angezeigt.

AutoUpdate aktualisiert das Produkt mit den neuesten DAT-Dateien, Spamregeln, Spam- und Antivirusmodulen der McAfee HTTP/FTP-Website.

Sie können den Aktualisierungstask auch über die Option **ePolicy Orchestrator-Agentenaktualisierung** im Dialogfeld **Task planen** planen.

Scannen auf Anforderung-Task

GroupShield für Exchange kann Scans auf Anforderung ausführen, sodass alle E-Mails auf dem Computer auf Viren, Trojanische Pferde und andere schädliche Codes geprüft werden. Sie können eine beliebige Anzahl von Plänen für das Scannen auf Anforderung erstellen. Die Scanpläne können vom Benutzer zu einem beliebigen Zeitpunkt ausgeführt und darüber hinaus so konfiguriert werden, dass die Scanvorgänge in bestimmten Intervallen gestartet werden. Zeitpläne, die nicht automatisch ausgeführt werden sollen, können zudem deaktiviert werden.

Erstellen eines neuen Tasks

1 Melden Sie sich mit einem Administratorkonto beim ePolicy Orchestrator-Server an.

2 Klicken Sie in der Konsolenstruktur unter **ePolicy Orchestrator** mit der rechten Maustaste auf **Verzeichnis** oder den gewünschten Standort, die Gruppe bzw. den Computer, und wählen Sie die Option **Task planen** aus.
Alternativ können Sie auch im oberen Detailbereich auf die Registerkarte **Tasks** klicken. Klicken Sie dann mit der rechten Maustaste auf den Bereich, und wählen Sie **Task planen** Das Dialogfeld **Task planen** wird geöffnet.

3 Geben Sie in das entsprechende Feld den Namen des neuen Tasks ein.

4 Wählen Sie in der Dropdown-Liste **Task-Typ** die Option **GroupShield for Exchange 7.0 Task auf Anforderung** aus.

5 Klicken Sie auf **OK**. Der erstellte Task wird auf der Registerkarte **Tasks** aufgelistet.

6 Senden Sie eine Agentenreaktivierung.

Weitere Informationen zum Senden einer Agentenreaktivierung finden Sie unter *Senden einer Agentenreaktivierung auf Seite 53*.

Bearbeiten eines Tasks

1 Klicken Sie mit der rechten Maustaste auf den Task, und wählen Sie die Option **Task bearbeiten** aus. Der **ePolicy Orchestrator-Planer** wird geöffnet.

2 Klicken Sie auf **Einstellungen**. Die Seite zum Konfigurieren von Scans auf Anforderung wird geöffnet.

3 Deaktivieren Sie das Kontrollkästchen **Vererben**.

4 Wählen Sie die gewünschte Auf Anforderungs-Richtlinie in der Liste aus:

5 Klicken Sie auf **OK**.

Planen von Einstellungen

6 Klicken Sie auf die Registerkarte **Zeitplan**.

Tabelle 5-2 Planungsoptionen

Task planen	Wählen Sie in der Dropdown-Liste einen Task-Typ aus. ■ **Täglich** ■ **Wöchentlich** ■ **Monatlich** ■ **Einmal** ■ **Bei Systemstart** ■ **Bei Anmeldung** ■ **Bei Leerlauf** ■ **Sofort ausführen** ■ **Bei Einwahl ausführen**
Startzeit ■ **UTC-Zeit** ■ **Ortszeit**	■ Geben Sie den Zeitpunkt für den Start des geplanten Tasks an. Wählen Sie die Ortszeit aus, um den Task in festgelegten Intervallen auf Basis der Systemzeit des Client-Computers auszuführen. Dies ist insbesondere bei Tasks sinnvoll, die größere Prozessorressourcen beanspruchen (z. B. Scans auf Anforderung), um derartige Tasks außerhalb der regulären Arbeitszeit auszuführen. ■ Bei Auswahl der Option **UTC-Zeit** wird die Koordinierte Weltzeit (entspricht der Greenwich Mean Time oder GMT) für die Ausführung des Tasks verwendet. Diese Option führt dazu, dass der Task auf allen Client-Systemen zur selben Zeit ausgeführt wird, unabhängig von der Ortzeit auf den einzelnen Client-Computern.
Zufallsgenerator	Der Task wird nicht zu einem festen Zeitpunkt ausgeführt. Stattdessen startet er nach einer zufällig ausgewählten Zeit. Geben Sie die gewünschte Zeitspanne in Stunden und Minuten für den Zufallsgenerator an.

Tabelle 5-2 Planungsoptionen

Verfehlten Task ausführen	Stellen Sie sicher, dass der Task gestartet wurde, wenn der Computer zum Zeitpunkt des geplanten Scans ausgeschaltet oder anderweitig nicht bereit ist. Wählen Sie diese Option aus, damit der Task ausgeführt wird, sobald der Computer wieder bereit ist.
Verfehlten Task verzögert ausführen	Klicken Sie im Dialogfeld **Erweiterte Planungsoptionen** auf **Erweitert**. Wenn diese Option ausgewählt ist, werden verfehlte Tasks verzögert ausgeführt, nachdem der Computer wieder bereit ist.
Startdatum/Enddatum	Klicken Sie im Dialogfeld **Erweiterte Planungsoptionen** auf **Erweitert**. Geben Sie das Start- und Enddatum ein, wenn der Task nur innerhalb eines bestimmten Zeitraums (Tage, Wochen) ausgeführt werden soll.
Task wiederholen	Klicken Sie im Dialogfeld **Erweiterte Planungsoptionen** auf **Erweitert**. Verwenden Sie diese Option, um einen Task mehrfach pro Tag auszuführen. Aktivieren Sie dafür das Kontrollkästchen **Task wiederholen**, und legen Sie das Wiederholungsintervall fest. Diese Option ist beispielsweise sinnvoll, um einen Client-Aktualisierungstask mehrmals täglich auszuführen, wenn viele neue Viren im Umlauf sind. Sie können auch andere Intervalle für eine Wiederholung einstellen, z. B. wöchentlich oder monatlich.
Task planen: Täglich	Geben Sie das Intervall an, um den Task auszuführen; dies können ein (1) oder mehrere Tage sein. Wenn Sie **1** einstellen, wird der Task alle zwei Tage ausgeführt.

Berichte

Über die ePolicy Orchestrator-Konsole können Sie Berichte anzeigen, in denen die Behandlung von Infektionen auf Client-Computern, auf denen GroupShield für Exchange installiert ist, dokumentiert wird. Außerdem können Sie die Konfiguration der Hosts prüfen. Sie können die im Dialogfeld **Berichtsdatenfilter** ausgewählten Optionen zur späteren Verwendung speichern.

ePolicy Orchestrator-Berichte bieten Ihnen folgende Möglichkeiten:

Legen Sie einen Verzeichnisfilter zur Sammlung der Informationen fest, die Sie anzeigen möchten. Wenn Sie diesen Filter festlegen, können Sie auswählen, welcher Teil der ePolicy Orchestrator-Konsolenstruktur in den Bericht einbezogen werden soll.

- Legen Sie unter Verwendung logischer Operatoren einen Datenfilter zur Definition präziser Filter für die Daten fest, die vom Bericht zurückgegeben werden.
- Erstellen Sie grafische Berichte aus den Informationen in der Datenbank, und filtern Sie die Berichte Ihren Anforderungen entsprechend. Berichte lassen sich ausdrucken und zur Weiterverwendung in andere Software exportieren.

Ausführen eines Berichts

1 Melden Sie sich bei dem ePolicy Orchestrator-Datenbankserver unter dem Abschnitt **Berichtserstellung** an.

2 Wählen Sie den gewünschten **GroupShield für Exchange 7.0**-Bericht unter **Berichtserstellung** | **ePO-Datenbanken** | **<Datenbankserver>** | **Berichte** | **<Produktname>** in der Konsolenstruktur aus. Das Dialogfeld **Berichtsdatenfilter festlegen** wird angezeigt.

- Bei Auswahl von **Ja** wird das Dialogfeld **Berichtsdatenfilter** für diese Kategorie angezeigt.
  Wählen Sie den Bericht (Agentenversionen) aus, den Sie erstellen möchten, und richten Sie dann den Datenfilter im Dialogfeld **Berichtsdatenfilter** ein. Klicken Sie auf **OK**.
- Bei Auswahl von **Nein** wird der gesamte Bericht angezeigt.

Je nach ausgewähltem Bericht werden unterschiedliche Registerkarten angezeigt. Weitere Informationen zu den verfügbaren Registerkarten finden Sie im *ePolicy Orchestrator v 3.6-Produkthandbuch*.

Konfigurieren von Berichten

Es gibt verschiedene Möglichkeiten zur Steuerung der Anzeige von Daten in Berichten. Sie können die Versionsnummer der Virusdefinitionsdateien, Scanmodule und unterstützte Produkte definieren, die auf Client-Computern installiert werden müssen, damit diese auf Grundlage des Virenschutz- und Sicherheitsprogramms Ihres Unternehmens als kompatibel angesehen werden. Sie können auch die Ergebnisse von Berichten mithilfe ausgewählter Produktkriterien einschränken. (Zum Beispiel Computername, Betriebssystem, Virusname oder für infizierte Dateien durchgeführte Maßnahme.) Wenn die Ergebnisse eines Berichts angezeigt werden, können Sie eine Reihe von Tasks mit den Daten ausführen. Sie können die Details erforderlicher Berichtsdaten anzeigen. (Um beispielsweise festzustellen, welche Client-Computer nicht über eine kompatible GroupShield-Version verfügen.) Einige Berichte enthalten sogar Links zu anderen Berichten, so genannten Unterberichten, die ergänzende Daten für den übergeordneten Bericht enthalten. Sie können Berichte außerdem ausdrucken und die Berichtsdaten in eine Reihe von Dateiformaten exportieren, darunter HTML und Microsoft® Excel.

Weitere Informationen zum Konfigurieren von Berichten finden Sie im *ePolicy Orchestrator v 3.6-Produkthandbuch*.

Deinstallation

Entfernen von GroupShield für Exchange vom Client-Computer

Mithilfe des ePolicy Orchestrator-Servers können Sie die auf dem Client-Computer installierte GroupShield-Software deinstallieren.

Entfernen der GroupShield-Software vom Client-Computer

1 Wählen Sie in der ePolicy Orchestrator-Konsole den **Standort** oder den Exchange-Server aus, auf dem GroupShield deinstalliert werden soll, und klicken Sie auf die Registerkarte **Tasks**. Die Seite **Ausbringungs-Task** wird angezeigt.

2 Doppelklicken Sie auf den **Ausbringungs-Task**. Daraufhin wird das Dialogfeld **ePolicy Orchestrator-Planer** angezeigt.

3 Deaktivieren Sie auf der Registerkarte **Tasks** das Kontrollkästchen **Vererben**, und wählen Sie die Option **Aktivieren (geplanter Task wird zu festgelegter Zeit ausgeführt)** aus.

4 Klicken Sie auf der Registerkarte **Tasks** auf **Einstellungen**. Die Seite **Taskeinstellungen** wird angezeigt.

5 Deaktivieren Sie das Kontrollkästchen **Vererben**. Wählen Sie in der Produktliste für den Eintrag **GroupShield für Exchange** die Aktion **Entfernen** aus.

6 Deaktivieren Sie das Kontrollkästchen **Diesen Task bei jedem Richtlinienumsetzungsintervall ausführen**.

7 Klicken Sie auf **OK**.

8 Klicken Sie auf die Registerkarte **Zeitplan**. Deaktivieren Sie das Kontrollkästchen **Vererben**.

9 Wählen Sie bei **Task planen** die Option **Sofort ausführen** aus, und klicken Sie auf **Übernehmen**.

10 Senden Sie eine Agentenreaktivierung.

Weitere Informationen zum Senden einer Agentenreaktivierung finden Sie unter *Senden einer Agentenreaktivierung auf Seite 53*.

Entfernen von GroupShield für Exchange aus ePolicy Orchestrator

Entfernen des Ausbringungspakets auf dem ePolicy Orchestrator-Server

1. Melden Sie sich mit einem Administratorkonto beim ePolicy Orchestrator-Server an.
2. Wählen Sie in der Konsolenstruktur **Repository** | **Software-Repositorys** | **Master** aus.
3. Wählen Sie **GroupShield für Exchange**, und klicken Sie auf **Löschen**. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie auf **OK**, um GroupShield für Exchange auf dem ePolicy Orchestrator-Server zu entfernen.

Entfernen der Produkt-NAP-Datei

1. Melden Sie sich mit einem Administratorkonto beim ePolicy Orchestrator-Server an.
2. Wählen Sie in der Konsolenstruktur **Repository** | **Verwaltete Produkte** | **Windows** | **GroupShield für Exchange** aus.
3. Klicken Sie mit der rechten Maustaste auf **7.0**, und wählen Sie **Entfernen** aus, um **GroupShield NAP** auf dem ePolicy Orchestrator-Server zu deinstallieren.

Entfernen der Berichts-NAP-Datei

1. Melden Sie sich mit einem Administratorkonto beim ePolicy Orchestrator-Server an.
2. Wählen Sie in der Konsolenstruktur **Berichtserstellung** | **Bericht-Repository** | **GroupShield 7.0** aus.
3. Klicken Sie mit der rechten Maustaste auf **GroupShield 7.0**, und wählen Sie **Entfernen** aus, um die Berichtsdatei auf dem ePolicy Orchestrator-Server zu deinstallieren.

6 Integrieren in ePolicy Orchestrator 4.0

Einführung

In diesem Kapitel wird die Konfiguration von GroupShield für Exchange mithilfe der Verwaltungssoftware McAfee ePolicy Orchestrator Version 4.0 erläutert. Damit Sie dieses Kapitel richtig einsetzen können, sollten Sie mit den Funktionen von ePolicy Orchestrator 4.0 vertraut sein.

ePolicy Orchestrator 4.0 bietet eine skalierbare Plattform für die zentrale Verwaltung und Durchsetzung von Richtlinien für Sicherheitsprodukte und Systeme.
Diese Lösung umfasst ebenfalls Funktionen zur umfassenden Berichterstellung und Produktausbringung. Alle Funktionen werden von einer zentralen Stelle aus gesteuert.

Dieses Handbuch enthält keine ausführlichen Informationen zum Installieren oder zum Einsatz von ePolicy Orchestrator. Weitere Informationen hierzu finden Sie im *Produkthandbuch von ePolicy Orchestrator*.

Voraussetzungen für die Installation von ePolicy Orchestrator

Installieren Sie für die Microsoft® Windows 2000-Plattform die folgenden Dateien auf Ihrem System:

- **dotnetfx.exe**
- **msxml6-KB925673-enu-x86.exe**
- **WindowsInstaller-KB893803-v2-x86.exe**

Installieren Sie für die Microsoft® Windows 2003-Plattform die folgenden Dateien auf Ihrem System:

- **dotnetfx.exe**
- **msxml6-KB925673-enu-x86.exe**

Bevor Sie beginnen

1 Erstellen Sie ein temporäres Verzeichnis im Netzwerk oder auf dem lokalen Laufwerk.

2 Für die Installation führen Sie einen der folgenden Schritte aus, abhängig davon, wie Sie die Software erhalten haben:

- Legen Sie die CD-ROM in das Laufwerk des Computers ein, und kopieren Sie die ZIP-Dateien in das erstellte temporäre Verzeichnis.
- Laden Sie die ZIP-Dateien in das temporäre Verzeichnis.

ePolicy Orchestrator-Agent

ePolicy Orchestrator-Agent ist eine dezentrale Komponente von ePolicy Orchestrator, die auf allen Computern im Netzwerk installiert werden muss. Der Agent sammelt und sendet Daten zwischen ePolicy Orchestrator-Server und Repositorys und verwaltet netzwerkweit Installationen von GroupShield für Exchange.

Voraussetzungen für die Verwendung von ePolicy Orchestrator 4.0

Bevor Sie GroupShield für Exchange mit ePolicy Orchestrator verwalten können, müssen Sie den ePolicy Orchestrator-Agenten auf dem Computer installieren.

Hinzufügen von Systemen und Ausbringen von Agents für den ePolicy Orchestrator-Server

1 Melden Sie sich mit einem Administratorkonto beim ePolicy Orchestrator-Server an.

2 Klicken Sie auf **Neue Systeme**. Die Seite **Neue Systeme** wird angezeigt.

3 Wählen Sie unter **Wie füge ich Systeme hinzu?** die Option **Der aktuellen Gruppe (Meine Organisation) Agenten ausbringen und Gruppen hinzufügen** aus.

Wenn Sie Systeme ohne Ausbringung von Agenten hinzufügen möchten, wählen Sie die Option **Der aktuellen Gruppe (Meine Organisation) Systeme hinzufügen, aber keine Agenten ausbringen** aus. Führen Sie die folgenden Schritte unter *Ausbringen eines ePolicy Orchestrator-Agenten auf Seite 69* durch, um Agenten zu einem späteren Zeitpunkt auszubringen:

4 Klicken Sie unter **Hinzuzufügende Systeme** auf **Durchsuchen**, um die hinzuzufügenden Systeme zu suchen. Die Seite **Systeme suchen** wird angezeigt.

5 Wählen Sie eine **Domäne** aus dem Dropdown-Menü aus, in dem die Systeme enthalten sind, die Sie hinzufügen möchten.

6 Wählen Sie unter **Systeme in ausgewählter Domäne** die gewünschten Systeme aus.

Wenn Sie alle Systeme einer Domäne auswählen möchten, klicken Sie auf **Alle auf dieser Seite auswählen**.

7 Klicken Sie auf **OK**, um zur Eigenschaftenseite **Neue Systeme** zurückzukehren.

8 Wählen Sie die gewünschte **Agentenversion** aus dem Dropdown-Menü aus, und legen Sie die **Installationsoptionen** und den **Installationspfad** fest.

9 Geben Sie die Benutzerinformationen (**Domäne Benutzer** und **Kennwort**) für die Agenteninstallation ein, und klicken Sie auf **OK**.

Ausbringen eines ePolicy Orchestrator-Agenten

1 Melden Sie sich mit einem Administratorkonto beim ePolicy Orchestrator-Server an.

2 Klicken Sie auf **Systeme**.

3 Wählen Sie im **Systemverzeichnis** eine Gruppe aus.

4 Wählen Sie **Computername** für diese Gruppe aus.

5 Klicken Sie auf **Agent ausbringen**. Auf der Seite **McAfee-Sicherheitsagent** werden die **Zielsysteme** angezeigt.

6 Wählen Sie eine auf den ausgewählten Systemen zu installierende **Agentenversion** aus.

Die in den Dropdown-Menüs verfügbaren Agentenmenüs richten sich nach dem Agenten, in das die Installationspakete eingecheckt wurden.

7 Wählen Sie die gewünschten **Installationsoptionen** und den **Installationspfad**, mit dem Sie den Agenten installieren möchten.

8 Geben Sie unter **Anmeldeinformationen für Agenteninstallation** die **Domäne**, den **Benutzer** und das **Kennwort** des Benutzerkontos an, mit dem Sie den Agenten auf den ausgewählten Systemen installieren möchten. Klicken Sie anschließend auf **OK**.

Installation

Einchecken des McAfee GroupShield für Microsoft Exchange Server 2003/2007-Pakets in den ePolicy Orchestrator-Server

Sie können das GroupShield für Exchange-Softwarpaket über die Seite **Master-Repository** einchecken. Das Master-Repository ist ein zentraler Speicherort für alle McAfee-Aktualisierungen auf dem ePolicy Orchestrator-Server. Dieses Repository ruft benutzerdefinierte Aktualisierungen von der McAfee-Site oder von benutzerdefinierten Quellsites ab.

1. Melden Sie sich mit einem Administratorkonto beim ePolicy Orchestrator-Server an.
2. Klicken Sie auf **Software** | **Paket einchecken**. Die Seite **Paket** wird angezeigt.
3. Wählen Sie den **Pakettyp** als **Product or Update (.ZIP)** (Produkt oder Aktualisierung im ZIP-Format) aus, und durchsuchen Sie den **Dateipfad** nach der in einem temporären Ordner gespeicherten Datei **GroupShield7_ePO4.zip.**
4. Klicken Sie auf **Weiter**. Auf der Seite **Paketoptionen** werden die **Paketinformationen** angezeigt.
5. Wählen Sie für **Ebene** den Eintrag **Aktuell** aus.
6. Klicken Sie auf **Speichern**.

Installieren von GroupShield für Exchange auf dem Clientcomputer

1. Melden Sie sich mit einem Administratorkonto beim ePolicy Orchestrator-Server an.
2. Klicken Sie auf **Systeme** | **Systemverzeichnis**, und wählen Sie die gewünschte Gruppe aus.
3. Klicken Sie auf der Registerkarte **Client-Tasks** auf **Task erstellen**.
4. Geben Sie einen **Namen** und **Hinweise** für den Task ein, und wählen Sie als **Typ** den Eintrag **Product Deployment (McAfee Agent 4.0.0)**.
5. Klicken Sie auf **Weiter**. Die Seite **Client-Taskerstellung** wird angezeigt.
6. Wählen Sie unter **Beschreibung** für **Zielplattform** den Eintrag **Windows** aus, um das Paket zu installieren.
7. Wählen Sie die gewünschte **Sprache** im Dropdown-Menü aus.

8 Wählen Sie unter **Auszubringendes Produkt** das Produkt **GroupShield für Exchange 7.0.0** aus der Dropdown-Liste aus, und legen Sie als **Aktion** die Option **Installieren** fest.

9 Aktivieren oder deaktivieren Sie unter **Optionen** die folgenden Optionen:

- **Diesen Task bei jedem Richtlinienumsetzungsintervall ausführen (nur Windows)**
- **Update nach erfolgreicher Produktausbringung (4.0 oder höher) ausführen**

10 Klicken Sie auf **Weiter**, um diesen Task wie gewünscht zu planen.

11 Klicken Sie auf **Weiter**, um eine Taskzusammenfassung anzuzeigen. Klicken Sie anschließend auf **Speichern**.

12 Wählen Sie auf der Registerkarte **Systeme** eine Gruppe und einen Computer aus, auf dem Sie GroupShield 7.0 installieren möchten.

Sie können alle Computer in einer Gruppe auswählen, um GroupShield 7.0 zu installieren. Klicken Sie hierzu auf **Alle auf der Seite auswählen**.

13 Senden Sie eine Agenten-Reaktivierung.

Weitere Informationen zum Senden einer Agentenreaktivierung finden Sie unter *Senden einer Agentenreaktivierung auf Seite 76*.

Erweiterungen

Sie können die GroupShield für Exchange-Erweiterungsdateien installieren, entfernen und verwalten. Erweiterungsdateien sind ZIP-Dateien, die installiert werden müssen, bevor dieses Produkt oder diese Komponente von ePolicy Orchestrator 4.0 verwaltet werden kann. Erweiterungsdateien für GroupShield für Exchange:

- **GROUPSHD7000.ZIP**
- **GSE7REPORTS.ZIP**

So installieren Sie die Erweiterungsdateien für die GroupShield für Exchange-Richtlinie

1 Melden Sie sich mit einem Administratorkonto beim ePolicy Orchestrator-Server an.

2 Klicken Sie auf **Konfiguration** | **Erweiterungen** | **Erweiterung installieren**. Das Dialogfeld **Erweiterung installieren** wird angezeigt.

3 Klicken Sie auf **Durchsuchen**, wählen Sie die Erweiterungsdatei **GROUPSHD7000.ZIP** aus, und klicken Sie auf **OK**.

So installieren Sie die Erweiterungsdateien für GroupShield für Exchange-Berichte

1. Melden Sie sich mit einem Administratorkonto beim ePolicy Orchestrator-Server an.
2. Klicken Sie auf **Konfiguration** | **Erweiterungen** | **Erweiterung installieren**. Das Dialogfeld **Erweiterung installieren** wird angezeigt.
3. Klicken Sie auf **Durchsuchen**, wählen Sie die Erweiterungsdatei **GSE7REPORTS.ZIP** aus, und klicken Sie auf **OK**.

Einführung von ePolicy Orchestrator 4.0 Dashboard

Dashboards stellen eine Sammlung an vorkonfigurierten und/oder benutzerdefinierten Monitoren dar, in denen aktuelle Daten über Ihre Erkennungen angezeigt werden.

Das ePolicy Orchestrator-Dashboard beinhaltet eine Sammlung an benannten Dashboardmonitoren. Je nach dem, welche Berechtigungen Ihrem Benutzerkonto zugewiesen sind, können Sie ein neues Dashboard erstellen, vorhandene Dashboards verwalten, aktive Dashboards auswählen und Dashboardeinstellungen bearbeiten.

Erstellen eines neuen Dashboards

1. Melden Sie sich mit einem Administratorkonto beim ePolicy Orchestrator-Server an.
2. Klicken Sie auf **Dashboards** | **Optionen** | **Neues Dashboard**. Die Seite **Neues Dashboard** wird angezeigt.
3. Geben Sie einen **Dashboardname** ein, und wählen Sie die gewünschte **Dashboardgröße** aus dem Dropdown-Menü aus.
4. Klicken Sie auf **Neuer Monitor**.
5. Wählen Sie als **Kategorie** den Eintrag **Abfragen** und eine auf GroupShield für Exchange bezogene Abfrage aus dem Dropdown-Menü **Monitor** aus.
6. Klicken Sie auf **OK**.
7. Wiederholen Sie die die Schritte 4 und 5 für die verbleibenden Monitore.
8. Klicken Sie auf **Ja**. Das Dialogfeld **Aktivieren** wird angezeigt.

9 Klicken Sie auf **Ja**, um das neue Dashboard zu Ihrem aktiven Satz hinzuzufügen.

Tabelle 6-1 Dashboardoptionen

Optionen	Beschreibung
Dashboardname	Gibt den Namen des ausgewählten Dashboards an.
Dashboardgröße	Gibt die Dimensionen (Anzahl der Dashboardmonitore) des ausgewählten Dashboards an.
Erstellt von	Gibt den Benutzernamen der Person an, die das ausgewählte Dashboard erstellt hat.
Zuletzt geändert von	Gibt den Benutzernamen, das Datum und den Zeitstempel der letzten Änderung an, die am ausgewählten Dashboard vorgenommen wurde.
Bearbeiten	Ruft die Seite **Dashboard bearbeiten** auf, auf der Sie den Namen und die Größe des Dashboards ändern können.
Löschen	Löscht das ausgewählten Dashboard.
Verdoppeln	Erstellt und speichert eine Kopie des ausgewählten Dashboards. Mit dieser Option können Sie ähnliche Dashboards erstellen und bearbeiten, ohne ein komplett neues Dashboard erstellen zu müssen.
Veröffentlichen	Fügt das ausgewählte private Dashboard der Liste der öffentlichen Dashboards hinzu. Alle Benutzer mit Zugriff auf öffentliche Dashboards können somit auf dieses Dashboard zugreifen.
Aktivieren	Fügt das ausgewählte Dashboard der Dashboards-Registerkarte hinzu, um den Zugriff zu erleichtern.

Berichterstellung

Berichte sind vorkonfigurierte Abfragen für die ePolicy Orchestrator-Datenbank mit einer grafischen Ausgabe.

ePolicy Orchestrator 4.0 beinhaltet eigene Abfrage- und Berichterstellungsfunktionen. McAfee bringt einen Reihe von Standardabfragen im linken Fensterbereich aus. Sie können jedoch eine neue Abfrage erstellen und alle Abfragen bearbeiten und verwalten.

Ausführen einer Abfrage

1. Melden Sie sich mit einem Administratorkonto beim ePolicy Orchestrator-Server an.
2. Klicken Sie auf **Berichterstellung**. Im linken Fensterbereicht wird eine Abfrageliste angezeigt.
3. Wählen Sie eine auf GroupShield für Exchange bezogene Abfrage aus der Liste aus.
4. Klicken Sie auf **Ausführen**. Die grafische Ausgabe wird angezeigt.

Erstellen einer neuen Abfrage

Wenn die vordefinierte Abfrage auf der linken Seite nicht zweckdienlich ist, können Sie in ePolicy Orchestrator Ihre eigenen Abfragen erstellen.

1. Melden Sie sich mit einem Administratorkonto beim ePolicy Orchestrator-Server an.
2. Klicken Sie auf **Berichterstellung** | **Neue Abfrage**. Die Seite **Ergebnistyp** wird geöffnet.
3. Wählen Sie im linken Fensterbereich den gewünschten Datentyp für die Abfrage aus, und klicken Sie auf **Weiter**. Die Seite **Diagramm** wird angezeigt.
4. Wählen Sie ein Diagramm bzw. eine Tabelle aus, und konfigurieren Sie sie entsprechend. Klicken Sie anschließend auf **Weiter**.
5. Auf der anschließend angezeigten Seite **Spalten** können Sie Spalten aus dem Diagramm bzw. aus der Tabelle auswählen.
6. Wählen Sie im Bereich **Verfügbare Spalten** die gewünschten Spalten aus, und klicken Sie auf **Weiter**.

7 Die Seite **Filter** wird angezeigt. Geben Sie die Kriterien an, indem Sie die Eigenschaften und Operatoren zum Beschränken der Daten, die durch die Abfrage abgerufen werden, auswählen.

8 Klicken Sie auf **Ausführen** und dann auf **Speichern**. Die Seite **Abfrage speichern** wird angezeigt.

9 Geben Sie einen **Name** und bei Bedarf **Hinweise** für die Abfrage ein, und klicken Sie auf **Speichern**.

Tabelle 6-2 Berichtsoptionen

Optionen	Beschreibung
Löschen	Löscht die ausgewählte Abfrage.
Bearbeiten	Startet die mit den Details der ausgewählten Abfrage erstellte Seite **Abfrageerstellung**, auf der Sie die Details der ausgewählten Abfrage bearbeiten können.
Veröffentlichen	Verschiebt die ausgewählte Abfrage von der Liste **Meine Abfragen** in die Liste **Öffentliche Abfragen**, so dass alle autorisierten Benutzer darauf zugreifen können.
Verdoppeln	Erstellt und speichert eine Kopie der ausgewählten Abfrage.
Exportieren	Exportiert die ausgewählte Abfrage in eine XML-Datei, die von einem beliebigen ePolicy Orchestrator-Server importiert werden kann.
Ausführen	Führt die ausgewählte Abfrage aus, und zeigt die jeweiligen Ergebnisse an.
Weitere Aktionen | Abfrage-SQL anzeigen	Öffnet die Seite **Abfrage-SQL anzeigen**, auf der Sie das SQL-Skript der ausgewählten Abfrage anzeigen und kopieren können.
Abfrage importieren	Öffnet ein Dialogfeld, in dem Sie zur exportierten Abfragedatei navigieren können. Beim Importieren einer Abfragedatei wird diese vom Server der Liste **Meine Abfragen** hinzugefügt.

Systeme

Alle Systeme im Netzwerk werden auf der Registerkarte **Systeme** verwaltet. Der **Systemverzeichnis** enthält alle Systeme, die von ePolicy Orchestrator verwaltet werden. Dieses Verzeichnis stellt die primäre Schnittstelle zum Verwalten von Richtlinien und Tasks auf diesen Systemen dar. Diese Systeme können im **System Tree** in logische Gruppen aufgeteilt und darin organisiert werden.

Meine Organisation stellt hierbei den Stamm des **System Tree** dar. Dieses Verzeichnis beinhaltet die Gruppe **Verloren&Gefunden**, in der Systeme gespeichert sind, die vom Server nicht gefunden werden. Je nach dem, welche Methode Sie zum Erstellen und Verwalten der **System Tree**-Segmente (Systeme) einsetzen, verwendet der Server verschiedene Merkmale zum Platzieren des Systems im **System Tree**.

Weitere Informationen zum Hinzufügen eines neuen Systems finden Sie im *Produkthandbuch für ePolicy Orchestrator 4.0*.

Senden einer Agentenreaktivierung

1. Melden Sie sich mit einem Administratorkonto beim ePolicy Orchestrator-Server an.
2. Klicken Sie auf **Systeme**.
3. Wählen Sie im **Systemverzeichnis** eine Gruppe aus.
4. Wählen Sie **Computername** für diese Gruppe aus.
5. Klicken Sie auf **Weitere Aktionen** | **Reaktivierungs-Agent**. Die Seite **Wake Up Agents** wird angezeigt.
6. Wählen Sie einen **Reaktivierungstyp** und einen Zeitraum für die **Zufallsgenerierung** von 0 bis 60 Minuten als Reaktion der Systeme auf die vom ePolicy Orchestrator gesendete Reaktivierung aus.
7. Aktivieren Sie für die Agenten das Kontrollkästchen **Alle Produkteigenschaften erhalten**, um nicht nur die Eigenschaften zu senden, die sich nach der letzten Kommunikation zwischen dem Server und dem Agenten geändert haben, sondern alle.
8. Klicken Sie auf **OK**.

Navigieren Sie zu **Protokoll für Server-Tasks**, um den Status der Agenten-Reaktivierung anzuzeigen.

Richtlinien

Im **Systemverzeichnis** können Sie eine Richtlinie erstellen, bearbeiten, löschen oder einer bestimmten Gruppe oder einem System zuweisen.

Erstellen einer neuen Richtlinie

1. Melden Sie sich mit einem Administratorkonto beim ePolicy Orchestrator-Server an.
2. Klicken Sie auf **Systeme** | **Systemverzeichnis**, und wählen Sie die gewünschte Gruppe aus.
3. Wählen Sie unter **Richtlinien** das gewünschte **Produkt** im Dropdown-Menü aus. Eine Liste der vom ausgewählten Produkt verwalteten Richtlinien wird im unteren Fensterbereich angezeigt.
4. Navigieren Sie zur gewünschten Richtlinienkategorie, und klicken Sie auf **Zuweisung bearbeiten**. Die Seite **Richtlinienzuweisung für: Meine Organsiation** | **Verloren&Gefunden** | **(ausgewählte Gruppe)** wird angezeigt.
5. Klicken Sie auf **Neue Richtlinie erstellen**. Das Dialogfeld **Neue Richtlinie erstellen** wird angezeigt.
6. Wählen Sie **McAfee-Standard** oder **Benutzerdefiniert** aus.

   Die Richtlinien für **McAfee Default** sind schreibgeschützt und können nicht bearbeitet, umbenannt oder gelöscht werden.

7. Geben Sie unter **Neuer Richtlinienname** einen Namen ein.
8. Klicken Sie auf **OK** und dann auf **Speichern**.

Durchsetzen von Richtlinien

Sie können eine Richtlinie für mehrere verwaltete Systeme innerhalb einer Gruppe durchsetzen.

1. Melden Sie sich mit einem Administratorkonto beim ePolicy Orchestrator-Server an.
2. Klicken Sie auf **Systeme** | **Systemverzeichnis**, und wählen Sie die gewünschte Gruppe aus.
3. Wählen Sie die gewünschten Systeme aus.
4. Klicken Sie auf **Richtlinie zuweisen**. Die Seite **Richtlinie für System x zuweisen** wird angezeigt.
5. Wählen Sie das gewünschte **Produkt**, die **Kategorie** und die **Richtlinie** aus dem Dropdown-Menü aus, und klicken Sie auf **Speichern**.
6. Wählen Sie die Systeme erneut aus.

7 Senden Sie eine Agentenreaktivierung.

Weitere Informationen zum Senden einer Agentenreaktivierung finden Sie unter *Senden einer Agentenreaktivierung auf Seite 76*.

Sie können GroupShield-Richtlinien nur erstellen und durchsetzen und Berichte anzeigen, nachdem die GroupShield-Erweiterungen hinzugefügt wurde.

Client-Tasks

Mit ePolicy Orchestrator können Sie Client-Tasks, die auf den verwalteten Systemen ausgeführt werden, erstellen, planen und verwalten. Client-Tasks können für den gesamten **Systemverzeichnis**, eine bestimmte Gruppe oder eine einzelnes System festgelegt werden.

Mit ePolicy Orchestrator 4.0 können Sie folgende geplante Tasks für GroupShield für Exchange erstellen:

- AutoUpdate
- Scan auf Anforderung

Die im Dropdown-Menü verfügbaren Client-Tasks richten sich nach den installierten Erweiterungsdateien.

AutoUpdate-Task

Ihre Software kann nur dann vollen Schutz bieten, wenn Sie die Virusdefinitionsdateien (DATs), die Anti-Spam-Regeln, das Anti-Spam-Modul und das Virenscanmodul regelmäßig aktualisieren. Es wird empfohlen, die DAT-Dateien täglich zu aktualisieren und regelmäßig die McAfee AVERT-Website (AVERT = Anti-Virus Emergency Response Team) auf neue DAT-Dateien zu überprüfen.

Erstellen eines neuen AutoUpdate-Tasks

1 Melden Sie sich mit einem Administratorkonto beim ePolicy Orchestrator-Server an.

2 Klicken Sie auf **Systeme** | **Systemverzeichnis**, und wählen Sie die gewünschte Gruppe aus.

3 Wählen Sie unter **Client-Tasks** die gewünschte Gruppe im **Systemverzeichnis**, für die Sie den Autoupdate-Task erstellen möchten.

4 Klicken Sie auf **Task erstellen**. Die Seite **Client-Taskerstellung** wird angezeigt.

5 Geben Sie unter **Beschreibung** einen **Name** und **Notizen** für den Autoupdate-Task ein.

6 Wählen Sie **AutoUpdate Task (GroupShield for Exchange 7.0.0)** als **Typ** für den Task aus, und klicken Sie auf **Weiter**.

7 Planen Sie den Task wie gewünscht, und klicken Sie auf **Weiter**, um die **Zusammenfassung** des Autoupdate-Task mit den folgenden Informationen für den Task anzuzeigen: **Name, Notizen, Produkt, Typ** und **Zeitplan**.

8 Klicken Sie auf **Speichern**.

9 Senden Sie eine Agenten-Reaktivierung.

Weitere Informationen zum Senden einer Agentenreaktivierung finden Sie unter *Senden einer Agentenreaktivierung auf Seite 76*.

Klicken Sie auf **Bearbeiten**, um die Beschreibung bzw. den Zeitplan für den Autoupdate-Task zu ändern, oder klicken Sie auf **Löschen**, um den Task zu entfernen.

Scannen auf Anforderung-Task

Sie können eine beliebige Anzahl von Plänen für das Scannen auf Anforderung erstellen. Die Scanpläne können vom Benutzer zu einem beliebigen Zeitpunkt ausgeführt und darüber hinaus so konfiguriert werden, dass die Scanvorgänge in bestimmten Intervallen gestartet werden.

Erstellen des Tasks „Scan auf Anforderung“

1. Melden Sie sich mit einem Administratorkonto beim ePolicy Orchestrator-Server an.
2. Klicken Sie auf **Systeme** | **Systemverzeichnis** | **Client-Tasks**.
3. Wählen Sie die gewünschte Gruppe im **Systemverzeichnis** aus, für die Sie den Task „Scan auf Anforderung“ erstellen möchten.
4. Klicken Sie auf **Task erstellen**. Die Seite **Client-Taskerstellung** wird angezeigt.
5. Geben Sie unter **Beschreibung** einen **Namen** und **Notizen** für den Task „Scan auf Anforderung“ ein.
6. Wählen Sie **On Demand Scan (GroupShield for Exchange 7.0.0)** als **Typ** für den Task aus, und klicken Sie auf **Weiter**.
7. Wählen Sie unter **Konfiguration** eine Richtlinie aus dem Dropdown-Menü aus.
8. Klicken Sie auf **Weiter**, um diesen Task wie gewünscht zu planen.
9. Klicken Sie auf **Weiter**, um die **Zusammenfassung** des Tasks „Scan auf Anforderung) mit den folgenden Informationen für den Task anzuzeigen: **Name**, **Notizen**, **Produkt**, **Typ** und **Zeitplan**.
10. Klicken Sie auf **Speichern**.
11. Senden Sie eine Agentenreaktivierung.

Weitere Informationen zum Senden einer Agentenreaktivierung finden Sie unter *Senden einer Agentenreaktivierung auf Seite 76*.

Klicken Sie auf **Bearbeiten**, um die Beschreibung bzw. den Zeitplan für den Task „Scan auf Anforderung“ zu ändern, oder klicken Sie auf **Löschen**, um den Task zu entfernen.

Deinstallation

Entfernen von GroupShield für Exchange auf dem Clientcomputer

1 Melden Sie sich mit einem Administratorkonto beim ePolicy Orchestrator-Server an.

2 Klicken Sie auf **Systeme** | **Systemverzeichnis**, und wählen Sie die gewünschte Gruppe aus.

3 Klicken Sie auf der Registerkarte **Client-Tasks** auf **Task erstellen**.

4 Geben Sie einen **Namen** und **Hinweise** für den Task ein, und wählen Sie als **Typ** den Eintrag **Product Deployment (McAfee Agent 4.0.0)**.

5 Klicken Sie auf **Weiter**. Die Seite **Client-Taskerstellung** wird angezeigt.

6 Wählen Sie unter **Beschreibung** für **Zielplattform** den Eintrag **Windows** aus, um das Paket zu deinstallieren.

7 Wählen Sie die gewünschte **Sprache** im Dropdown-Menü aus.

8 Wählen Sie unter **Auszubringendes Produkt** das Produkt **GroupShield für Exchange 7.0.0** aus der Dropdown-Liste aus, und legen Sie als **Aktion** die Option **Entfernen** fest.

9 Aktivieren oder deaktivieren Sie unter **Optionen** die folgenden Optionen:

- **Diesen Task bei jedem Richtlinienumsetzungsintervall ausführen (nur Windows)**
- **Update nach erfolgreicher Produktausbringung (4.0 oder höher) ausführen**

10 Klicken Sie auf **Weiter**, um diesen Task wie gewünscht zu planen.

11 Klicken Sie auf **Weiter**, um eine Taskzusammenfassung anzuzeigen. Klicken Sie anschließend auf **Speichern**.

12 Wählen Sie auf der Registerkarte **Systeme** eine Gruppe und einen Computer aus, auf dem Sie GroupShield 7.0 installieren möchten.

Sie können alle Computer in einer Gruppe auswählen, um GroupShield 7.0 zu installieren. Klicken Sie hierzu auf **Alle auf der Seite auswählen**.

13 Senden Sie eine Agenten-Reaktivierung.

Weitere Informationen zum Senden einer Agentenreaktivierung finden Sie unter *Senden einer Agentenreaktivierung auf Seite 76*.

Entfernen von GroupShield für Exchange vom ePolicy Orchestrator-Server

Entfernen des Ausbringungspakets von ePolicy Orchestrator

1. Melden Sie sich mit einem Administratorkonto beim ePolicy Orchestrator-Server an.
2. Klicken Sie auf **Software** | **Master Repository**.
3. Klicken Sie auf den Link **Löschen** des GroupShield für Exchange-Pakets.

Entfernen der Produkterweiterung

1. Melden Sie sich mit einem Administratorkonto beim ePolicy Orchestrator-Server an.
2. Klicken Sie auf **Konfiguration**.
3. Wählen Sie die Erweiterungsdatei **GroupShield für Exchange**, und klicken Sie auf **Entfernen**.
4. Wählen Sie die Option **Löschenvorgang unter Umgehung aller Prüfungen und Fehler erzwingen** aus.
5. Klicken Sie auf **OK**.

Entfernen der Berichtserweiterung

1. Melden Sie sich mit einem Administratorkonto beim ePolicy Orchestrator-Server an.
2. Klicken Sie auf **Konfiguration**.
3. Wählen Sie die Erweiterungsdatei für GroupShield für Exchange-Berichte aus, und klicken Sie auf **Entfernen**.
4. Wählen Sie die Option **Löschenvorgang unter Umgehung aller Prüfungen und Fehler erzwingen** aus.
5. Klicken Sie auf **OK**.

7 Integrieren in ProtectionPilot 1.5

Einführung

Die ProtectionPilot-Software ist ein Sicherheitsverwaltungssystem und vereinfacht Netzwerkadministratoren, die für bis zu 500 Computer zuständig sind, Virenschutz-Verwaltungstasks. Die Verwaltungsaufgaben umfassen die Bereitstellung (Senden und Installieren) von Virenschutzprodukten, die Konfiguration von Produkteinstellungen und die regelmäßige Aktualisierung dieser Produkte. Um GroupShield für Exchange mit ProtectionPilot zu verwalten, müssen Sie GroupShield in der Software registrieren und konfigurieren. Bei der ersten Anmeldung beim Server wird an der Konsole die aktuelle Sicherheitsstufe angezeigt. Dieses Handbuch beschreibt die Konfiguration von GroupShield für Exchange unter Verwendung von McAfee ProtectionPilot Version 1.5. Damit Sie dieses Handbuch richtig einsetzen können, sollten Sie mit den Funktionen von ProtectionPilot vertraut sein.

Dieses Handbuch enthält keine ausführlichen Informationen zum Installieren oder zum Einsatz von ProtectionPilot. Weitere Informationen finden Sie im *Produkthandbuch von ProtectionPilot v1.5*.

Voraussetzungen für die Verwendung von ProtectionPilot

Bevor Sie ProtectionPilot zur Konfiguration von GroupShield für Exchange verwenden können, müssen Sie folgende Schritte durchführen:

- Checken Sie das entsprechende Paket und die entsprechende NAP-Datei für GroupShield für Exchange im Software-Repository von ProtectionPilot ein.
- Installieren Sie den ProtectionPilot-Agenten auf Ihrem Computer.

Einführung in ProtectionPilot

Die Benutzerschnittstelle für den Zugriff auf ProtectionPilot basiert auf Microsoft® Management Console (MMC). Über die MMC-Schnittstelle registrieren und konfigurieren Sie die verschiedenen Produkte von GroupShield für Exchange, die sich über ProtectionPilot verwaltet werden. Die Konsole verwendet MMC-Standardfunktionen.

Die Konsole besteht aus zwei Bereichen. Wenn Sie sich zum ersten Mal am Server anmelden, wird das Konsolenstammverzeichnis im linken Bereich der Konsole hervorgehoben angezeigt.

- Die Konsolenstruktur ist der Navigationsbereich der Konsole. Darin werden die Server, Workstation und Anwendungen angezeigt, die Sie mithilfe von ProtectionPilot verwalten können.
- Im rechten Bereich der Konsole befindet sich der Detailbereich. Je nach ausgewähltem Element in der Konsolenstruktur kann der Detailbereich in einen oberen und einen unteren Detailbereich unterteilt sein.

Der Aufbau der Konsole ändert sich entsprechend den markierten Objekten in der Konsolenstruktur bzw. des Detailbereichs.

McAfee Common Agent dient zur Remote-Verwaltung von Produkten. Er wird auf jedem Computer installiert und ermöglicht die Bereitstellung von Produkten, die Aktualisierung der Virusdefinitionsdateien (DAT) und des Virenscanmoduls sowie Upgrades vorhandener Produkte mit Service Packs und Patches. Außerdem erfasst er Daten zu installierten Virenschutzprodukten, dem Computer, möglichen Infektionen und der Systemaktivität. Durch den Common Agent wird sichergestellt, dass Anforderungen des Servers ausgeführt, erneut ausgeführt oder nach Bedarf durchgesetzt werden. Wenn ein Benutzer beispielsweise das Virenschutzprodukt entfernt, das Sie für den Computer definiert haben, installiert der Agent das Produkt automatisch neu.

Annahme:

- Computer 1: ProtectionPilot ist auf einem Computer mit unterstütztem Betriebssystem installiert und konfiguriert.
- Computer 2: Microsoft® Exchange Server 2003 oder 2007 ist auf dem Server installiert und konfiguriert.
- Der Exchange-Server wird in die Liste der verwalteten Server von ProtectionPilot in die Verzeichnisebene aufgenommen.
- McAfee Common Agent ist auf dem ProtectionPilot-Server installiert.
- Der ProtectionPilot-Agent wird über die ProtectionPilot-Serverkonsole auf dem Exchange-Server installiert (herkömmliche oder Push-Installation).

Bevor Sie beginnen

1 Erstellen Sie ein temporäres Verzeichnis im Netzwerk oder auf dem lokalen Laufwerk.

2 Für die Installation führen Sie einen der folgenden Schritte aus, abhängig davon, wie Sie die Software erhalten haben:

- Legen Sie die CD-ROM in das Laufwerk des Computers ein, und kopieren Sie die Installationsdateien in das erstellte temporäre Verzeichnis.
- Laden Sie das NAP- und pkgCatalog.z-Archiv herunter, und extrahieren Sie die Datei in das temporäre Verzeichnis.

Die Anti-Spam- und Anti-Phishing-Funktionalität ist nur verfügbar, wenn Sie nach der Installation die Komponente McAfee Anti-Spam für GroupShield ausgewählt haben. Um die Anti-Spam- und Anti-Phishing-Funktionalität zu installieren, müssen Sie das erforderliche Paket in das Repository einchecken und dann implementieren. Wenn das Evaluierungspaket bereitgestellt ist und Sie auf die lizenzierte Version hochstufen möchten, müssen Sie das Lizenzpaket einchecken und implementieren.

Installation

Hinzufügen der Datei „pkgCatalog.z“ von McAfee GroupShield für Exchange zum ProtectionPilot-Server:

1 Ermitteln Sie den Speicherort der Datei **pkgCatalog.z**.

2 Melden Sie sich beim ProtectionPilot-Server als Administrator an.

3 Wählen Sie auf der Seite **Server** die Registerkarte **Repository** aus. Klicken Sie unter **Verwaltungstasks** auf **Paket einchecken**. Der Assistent für das Einchecken von Paketen wird geöffnet.

4 Wählen Sie **Produkte und Aktualisierungen** aus, und klicken Sie auf **Weiter**. Wählen Sie die Datei **pkgCatalog.z** für McAfee GroupShield für Exchange aus, die Sie in Schritt 1 in einem temporären Ordner gespeichert haben.

5 Klicken Sie auf **Öffnen**, damit ProtectionPilot die Paketdatei laden kann.

6 Klicken Sie auf **Fertig stellen**, damit ProtectionPilot die Datei **pkgCatalog.z** laden kann.

Hinzufügen der NAP-Datei von McAfee GroupShield für Exchange zum ProtectionPilot-Server:

1 Wählen Sie die NAP-Datei auf der Produkt-CD oder in der ZIP-Datei für die Installation aus, die Sie von der McAfee-Website heruntergeladen haben, und speichern Sie sie in einem temporären Ordner, auf den Sie über den ProtectionPilot-Server zugreifen können.

2 Melden Sie sich beim ProtectionPilot-Server als Administrator an.

3 Wählen Sie auf der Seite **Server** die Registerkarte **Repository** aus. Klicken Sie unter **Verwaltungstasks** auf **Paket einchecken**. Der Assistent für das Einchecken von Paketen wird geöffnet.

4 Wählen Sie **Verwaltungs-NAP** aus, und klicken Sie auf **Weiter**. Wählen Sie die Datei **GSEWIN70.nap** für McAfee GroupShield aus, die Sie in Schritt 1 in einem temporären Ordner gespeichert haben.

5 Klicken Sie auf **Fertig stellen**, damit ProtectionPilot die NAP-Datei laden kann.

Bereitstellen von McAfee GroupShield über den ProtectionPilot-Server:

1 Wählen Sie die erforderliche **Site**, die **Gruppe** oder den **Computer** im ProtectionPilot-Verzeichnis aus, und klicken Sie auf die Registerkarte **Tasks**.

2 Bearbeiten Sie den Task **Ausbringung**, um McAfee GroupShield für Exchange wie erforderlich zu installieren.

Konfigurieren von GroupShield-Richtlinien

In diesem Abschnitt erfahren Sie mehr über die Durchsetzung von Richtlinien mithilfe von ProtectionPilot. Es gibt zwei wichtige Schritte:

1 In ProtectionPilot können Sie die Namen der Zielcomputer im Netzwerk sowie die Richtlinien auswählen, die auf diese Computer angewendet werden sollen. Auf allen Zielcomputern ist der ProtectionPilot-Agent installiert. Sie können eine Reihe verschiedener Richtlinien festlegen, die auf mehrere einzelne Computer oder Gruppen von Computern angewendet werden.

2 Sie können ProtectionPilot zur Durchsetzung dieser Richtlinien auf den Computern konfigurieren. Der Agent kommuniziert mit dem Server, um ggf. neue Richtlinien abzufragen. Jeder Computer befolgt dann die neue Richtlinie. Bisherige mit GroupShield für Exchange konfigurierte Richtlinien werden ignoriert.

Einrichten und Durchsetzen von Richtlinien

Mithilfe der ProtectionPilot-Konsole können Sie Richtlinien für Gruppen von Computern oder einen einzelnen Computer durchsetzen. Diese Richtlinien setzen die Konfigurationseinstellungen der einzelnen Computer außer Kraft. Informationen bezüglich Richtlinien und ihrer Durchsetzung finden Sie im *ProtectionPilot-Produkthandbuch*.

Wählen Sie vor dem Konfigurieren von Richtlinien die Gruppe der Computer aus, deren GroupShield-Richtlinien Sie bearbeiten möchten. Sie können GroupShield-Richtlinien mithilfe der Seiten und Registerkarten bearbeiten, die im Detailbereich der ProtectionPilot-Konsole zur Verfügung stehen. Diese Seiten sind nahezu identisch mit jenen, auf die Sie direkt über die Benutzeroberfläche von GroupShield zugreifen können.

Nachdem Sie die entsprechenden Richtlinien geändert und die Änderungen für den gewünschten Computer bzw. die Gruppe von Computern gespeichert haben, können Sie die neuen Einstellungen über den ProtectionPilot-Agenten bereitstellen.

Ändern von Richtlinien für GroupShield mithilfe von ProtectionPilot

1. Melden Sie sich beim ProtectionPilot-Server an.
2. Wählen Sie in der Konsolenstruktur unter **McAfee ProtectionPilot** | **<SERVER>** | **Verzeichnis** den Pfad, die Gruppe, den einzelnen Computer oder das gesamte Verzeichnis aus, auf welches diese Richtlinien angewendet werden sollen.
3. Der Detailbereich enthält die Registerkarten **Allgemein**, **Richtlinien**, **Geplante Tasks** und **Agentenprotokoll**.
4. Klicken Sie auf **Richtlinien** und anschließend auf den Link **GroupShield für Exchange**. Die Seite **Richtlinieneinstellungen** wird mit der Standardrichtlinienkategorie **Scannereinstellungen** geöffnet.
5. Deaktivieren Sie das Kontrollkästchen **Vererbt**, und ändern Sie gegebenenfalls die Richtlinieneinstellungen.

Weitere Informationen zur Änderung der Richtlinieneinstellungen finden Sie *im Kapitel Richtlinien-Manager auf Seite 117*.

Einstellen der Fehlersuchprotokollierung

1. Melden Sie sich beim ProtectionPilot-Server an.
2. Wählen Sie in der Konsolenstruktur unter **McAfee ProtectionPilot** | **<SERVER>** | **Verzeichnis** den Pfad, die Gruppe, den einzelnen Computer oder das gesamte Verzeichnis aus, auf welches diese Richtlinien angewendet werden sollen.
3. Der Detailbereich enthält die Registerkarten **Allgemein**, **Richtlinien**, **Geplante Tasks** und **Agentenprotokoll**.

4 Klicken Sie auf **Richtlinien** und anschließend auf den Link **GroupShield für Exchange**.

5 Wählen Sie aus dem Dropdown-Menü die Option **Diagnose** aus. Die Seite **Diagnose** wird angezeigt.

6 Klicken Sie auf die Registerkarte **Fehlersuchprotokollierung**.

7 Wählen Sie die Ebene für die Fehlersuchprotokollierung aus:

- **Hoch** — Erfasst eine große Anzahl von Protokolleinträgen.
- **Mittel** — Erfasst eine mittlere Anzahl von Protokolleinträgen.
- **Niedrig** — Erfasst eine geringe Anzahl von Protokolleinträgen.
- **Ohne** — Deaktiviert die Fehlersuchprotokollierung.

8 Wählen Sie **Größenlimit für Fehlersuchprotokolldateien** aus, um anzugeben, ob ein Größenlimit für Fehlersuchprotokolldateien gelten soll. Sie können angeben, wie groß die Fehlersuchprotokolldateien maximal sein dürfen (in MB oder KB).

9 Wählen Sie **Pfad für Fehlersuchdateien angeben** aus, um festzulegen, ob Sie den Standardpfad für Fehlersuchdateien verwenden oder einen anderen Pfad angeben möchten. Wenn Sie einen neuen Pfad angeben, wählen Sie im ersten Feld die Art des Pfads aus, und geben Sie in das zweite Feld die Pfaddetails ein.

Einstellen des Fehlerberichterstellungsdienstes

1 Klicken Sie auf die Registerkarte **Fehlerberichterstellungsdienst**.

2 Wählen Sie **Aktivieren** aus, um den Fehlerberichterstellungsdienst zu aktivieren oder zu deaktivieren.

3 Wählen Sie **Ausnahmen abfangen** aus, um Informationen über Ausnahmeereignisse, wie z. B. Systemabstürze, zu erfassen.

4 Wählen Sie **Ausnahmen an Benutzer melden** aus, um anzugeben, ob Ausnahmen dem Administrator gemeldet werden sollen.

Einstellen der Ereignisprotokollierung

1 Klicken Sie auf die Registerkarte **Ereignisprotokollierung**, um anzugeben, welche Ereignisse in das **Produktprotokoll** und das **Ereignisprotokoll** einbezogen werden sollen.

2 Wählen Sie **Ereignisse vom Typ ‚Information' schreiben**, **Ereignisse vom Typ ‚Warnung' schreiben** oder **Ereignisse vom Typ ‚Fehler' schreiben** aus, um diese Art von Ereignissen in das Produktprotokoll aufzunehmen.

3 Wählen Sie **Ereignisse vom Typ ‚Information' schreiben**, **Ereignisse vom Typ ‚Warnung' schreiben** oder **Ereignisse vom Typ ‚Fehler' schreiben** aus, um diese Art von Ereignissen in das Ereignisprotokoll aufzunehmen.

Einstellen des Produktprotokolls

1 Klicken Sie auf die Registerkarte **Produktprotokoll**.

2 Wählen Sie **Pfad der Datenbank angeben** aus, um anzugeben, ob Sie den Standardpfad für das Produktprotokoll verwenden oder einen anderen Pfad angeben möchten. Wenn die Option deaktiviert ist, wird der Standardpfad verwendet.

3 Geben Sie den **Datenbankpfad** an, oder wählen Sie einen anderen Pfad für das Produktprotokoll aus. Wählen Sie im ersten Feld die Art des Pfads aus, den Sie im zweiten Feld angeben möchten. Wenn Sie beispielsweise im ersten Feld **Vollständiger Pfad** auswählen, geben Sie den Namen des vollständigen Pfads in das zweite Feld ein. Wenn Sie einen Pfad auswählen, geben Sie den Dateinamen oder den Unterverzeichnispfad und den Dateinamen an.

4 Wählen Sie die Option **Dateiname der Datenbank angeben** aus, um anzugeben, ob Sie den Standarddateinamen für die Datenbank verwenden oder einen anderen Namen angeben möchten. Wenn die Option deaktiviert ist, wird der Standarddateiname verwendet. Der Standarddateiname ist **productlog.bin**. Alternativ können Sie einen anderen Namen für das Produktprotokoll in das Feld **Datenbankdateiname** eingeben.

5 Wählen Sie **Datenbankgröße begrenzen** aus, um die Größe der Produktprotokolldatenbank einzugeben.

6 Geben Sie die **Maximale Datenbankgröße** für die Produktprotokolldatenbank ein. Die Größe kann entweder in Megabyte oder in Kilobyte angegeben werden.

7 Wählen Sie **Alterslimit für Einträge** aus, um anzugeben, dass Produktprotokolleinträge nach einem festgelegten Zeitraum gelöscht werden sollen.

8 Geben Sie durch die Eingabe unter **Maximales Eintragsalter** an, wie viele Tage ein Eintrag in der Datenbank verbleiben soll, bis er gelöscht wird.

9 Wählen Sie **Abfragezeitlimit angeben** aus, um die zulässige Zeitdauer für die Beantwortung einer Produktprotokollabfrage festzulegen.

10 Geben Sie das **Abfragezeitlimit (Sekunden)** ein, um die maximal zulässige Zeitdauer für die Beantwortung einer Produktprotokollabfrage in Sekunden anzugeben.

Planen von Tasks

In diesem Kapitel erfahren Sie mehr über die Durchsetzung von Richtlinien mithilfe von ProtectionPilot. GroupShield kann Scans auf Anforderung für den Exchange-Server durchführen.

Einstellungen und Aktionen können in Richtlinien für Scans auf Anforderung angegeben werden. Diese befinden sich unter **Richtlinien-Manager**. Für Tasks für Scans auf Anforderung stehen drei Richtliniensätze zur Verfügung. Diese sind:

- **Auf Anforderung (Viren entfernen):** Die Richtlinien in diesem Satz umfassen Virenschutzeinstellungen und Filter. Diese Richtlinien sind ein einfaches Mittel zur Überprüfung von Datenbanken auf mit Viren infizierte Inhalte.
- **Auf Anforderung (Gesperrte Inhalte entfernen):** Die Richtlinien in diesem Satz umfassen Einstellungen für Inhaltsscans. Diese Richtlinien sind insbesondere nützlich, wenn Sie die Auswirkungen neu erstellter/zugewiesener Regeln für Inhaltsscans testen möchten.
- **Auf Anforderung (Vollständiger Scan):** Die Richtlinien in diesem Satz umfassen Einstellungen für alle Scanner und Filter. Diese Richtlinien werden typischerweise für regelmäßige Scans verwendet.

Erstellen eines neuen Tasks zum Scannen auf Anforderung

1. Melden Sie sich beim ProtectionPilot-Server an.
2. Wählen Sie in der Konsolenstruktur unter **McAfee ProtectionPilot** | **<SERVER>** | **Verzeichnis** den Pfad, die Gruppe, den einzelnen Computer oder das gesamte Verzeichnis aus, auf welches diese Richtlinien angewendet werden sollen.
3. Der Detailbereich enthält die Registerkarten **Allgemein**, **Richtlinien**, **Geplante Tasks** und **Agentenprotokoll**.
4. Klicken Sie auf die Registerkarte **Geplante Tasks**. Die Seite **Geplante Tasks für Computer** <Computername> wird angezeigt.
5. Klicken Sie auf **Task erstellen**. Die Seite **Task-Typen** wird angezeigt.
6. Klicken Sie auf den Eintrag **GroupShield für Exchange** mit dem Task-Typ **Task für Scannen bei Bedarf**.
7. Klicken Sie auf **Weiter**. Die Seite **Taskeinstellungen** wird angezeigt.
8. Geben Sie einen Namen für den Task ein.
9. Deaktivieren Sie unter **Zeitplaneinstellungen** das Kontrollkästchen **Erbt**.
10. Wählen Sie die Option **Aktivieren (geplanter Task wird zu festgelegter Zeit ausgeführt)** aus, um Tasks für Scans auf Anforderung zu aktivieren.
11. Wählen Sie die nächste Option aus, wenn Sie den Task nach einer bestimmten Zeit beenden möchten. Geben Sie die Zeit in Stunden und Minuten an, nach der der Task gestoppt wird.
12. Wählen Sie zum Planen von Scanvorgängen aus der Dropdown-Liste einen Intervall aus. Für die Ausführung von Scanvorgängen haben Sie die Optionen **Sofort**, **Einmal**, **Stündlich**, **Täglich**, **Wöchentlich** oder **Monatlich**. Nehmen Sie gegebenenfalls Einstellungen für die gewählte Option vor.
13. Klicken Sie auf **Einstellungen übernehmen**. Der neu erstellte Task wird auf der Seite **Geplante Tasks** aufgelistet, wobei als Task-Typ **Task für Scannen bei Bedarf** angezeigt wird.

Wählen Sie den gewünschten Task aus, und klicken Sie auf **Bearbeiten**, um die Einstellungen zu ändern. Oder klicken Sie auf **Löschen**, um den Task zu entfernen, falls er nicht mehr benötigt wird.

Erstellen eines neuen AutoUpdate-Tasks

1. Melden Sie sich beim ProtectionPilot-Server an.
2. Wählen Sie in der Konsolenstruktur unter **McAfee ProtectionPilot** | **<SERVER>** | **Verzeichnis** den Pfad, die Gruppe, den einzelnen Computer oder das gesamte Verzeichnis aus, auf welches diese Richtlinien angewendet werden sollen.
3. Der Detailbereich enthält die Registerkarten **Allgemein**, **Richtlinien**, **Geplante Tasks** und **Agentenprotokoll**.
4. Klicken Sie auf die Registerkarte **Geplante Tasks**. Die Seite **Geplante Tasks für Computer** <Computername> wird angezeigt.
5. Klicken Sie auf **Task erstellen**. Die Seite **Task-Typen** wird angezeigt.
6. Klicken Sie auf den Eintrag **GroupShield 7.0 für Exchange** mit dem Task-Typ **AutoUpdate-Task**.
7. Klicken Sie auf **Weiter**. Die Seite **Taskeinstellungen** wird angezeigt.
8. Geben Sie einen Namen für den Task ein.
9. Deaktivieren Sie unter **Zeitplaneinstellungen** das Kontrollkästchen **Erbt**.
10. Wählen Sie die Option **Aktivieren (geplanter Task wird zu festgelegter Zeit ausgeführt)** aus, um Tasks für Scans auf Anforderung zu aktivieren.
11. Wählen Sie die nächste Option aus, wenn Sie den Task nach einer bestimmten Zeit beenden möchten. Geben Sie die Zeit in Stunden und Minuten an, nach der der Task gestoppt wird.
12. Wählen Sie zum Planen von Scanvorgängen aus der Dropdown-Liste einen Intervall aus. Für die Ausführung von Scanvorgängen haben Sie die Optionen **Sofort**, **Einmal**, **Stündlich**, **Täglich**, **Wöchentlich** oder **Monatlich**. Nehmen Sie gegebenenfalls Einstellungen für die gewählte Option vor.
13. Klicken Sie auf **Einstellungen übernehmen**. Der neu erstellte Task wird auf der Seite **Geplante Tasks** aufgelistet, wobei als Task-Typ **AutoUpdate-Task** angezeigt wird.

Wählen Sie den gewünschten Task aus, und klicken Sie auf **Bearbeiten**, um die Einstellungen zu ändern. Oder klicken Sie auf **Löschen**, um den Task zu entfernen, falls er nicht mehr benötigt wird.

Deinstallation

Entfernen von McAfee GroupShield für Exchange über den ProtectionPilot-Server vom Client-Computer

1. Wählen Sie die erforderliche **Site**, die **Gruppe** oder den **Computer** im ProtectionPilot-Verzeichnis aus.
2. Klicken Sie unter **Verwaltungstasks** auf **Produkte deinstallieren** und anschließend auf **Weiter**. Der Assistent zum Deinstallieren von Produkten wird angezeigt. Hier haben Sie die Möglichkeit, die Angaben zu **Produktname** und **Version** aus der ProtectionPilot-Konsole zu entfernen. Sie können GroupShield für Exchange auch vom Client-System deinstallieren, indem Sie den Eintrag **GroupShield für Exchange** aus der Liste auswählen.
3. Klicken Sie auf **Ja**, um die Installation zu entfernen.

Entfernen der Paketdatei „pkgCatalog.z“ für McAfee GroupShield für Exchange aus dem ProtectionPilot-Repository:

1. Melden Sie sich beim ProtectionPilot-Server als Administrator an.
2. Wählen Sie unter **Repository** | **Inhalte des Server-Repositories anzeigen** den Eintrag **GroupShield für Exchange** aus.
3. Wählen Sie als **Typ** die Option **Installation** aus. Wählen Sie anschließend aus der Liste **Inhalte des Server-Repositories anzeigen** den Eintrag **GroupShield für Exchange** aus.
4. Klicken Sie auf **Löschen**, um die Paketdatei für GroupShield für Exchange vom Server zu deinstallieren.

Entfernen der NAP-Datei für McAfee GroupShield für Exchange aus dem ProtectionPilot-Server

1. Melden Sie sich beim ProtectionPilot-Server als Administrator an.
2. Wählen Sie unter **Repository** | **Inhalte des Server-Repositories anzeigen** den Eintrag **GroupShield für Exchange** aus.
3. Wählen Sie als **Typ** die Option **NAP** aus. Wählen Sie anschließend aus der Liste **Inhalte des Server-Repositories anzeigen** den Eintrag **GroupShield für Exchange** aus.
4. Klicken Sie auf **Löschen** und anschließend auf **OK**, um die NAP-Datei für GroupShield für Exchange vom Server zu deinstallieren.

8 Erste Schritte in der Benutzeroberfläche

Die Benutzeroberfläche bietet wichtige Funktionen für GroupShield-Administratoren. Administratoren müssen genau wissen, wie gut ihr Server vor Viren und gesperrten Inhalten geschützt ist. Das Dashboard ist Ihre Verbindung zu GroupShield für Exchange.

Auf der linken Seite der Konsole werden Links wie **Dashboard**, **Erkannte Elemente**, **Richtlinien-Manager** und **Einstellungen und Diagnose** angezeigt, die Sie verwalten können. Im rechten Bereich werden Informationen zu dem Element angezeigt, das Sie im linken Bereich auswählen.

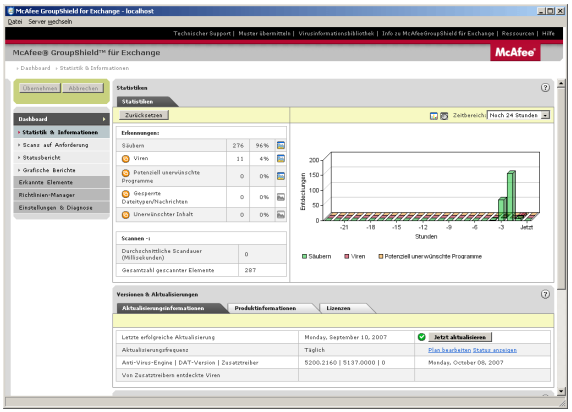
So öffnen Sie die Benutzeroberfläche von GroupShield für Exchange

1. Starten Sie **McAfee GroupShield für Exchange** über das Symbol auf dem Desktop.
2. Sie können GroupShield für Exchange ebenfalls starten, indem Sie auf **Start** | **Programme** | **McAfee** | **GroupShield für Exchange** klicken. Wählen Sie entweder **GroupShield für Exchange** oder **GroupShield für Exchange (Web)**.

Dashboard

Das Dashboard bietet eine Übersicht über die Details der Scanvorgänge, die neuesten Erkennungen, die grafische Darstellung dieser Erkennungen, Produktaktualisierungen und -versionen, eine Liste der zuletzt gescannten Elemente, Antivirus- und Sicherheitsnachrichten.

Abbildung 8-1 Dashboard



Das Dashboard enthält vier Seiten:

- *Statistik & Informationen*
- *Scans auf Anforderung*
- *Statusbericht*
- *Grafische Berichte*

Statistik & Informationen

Die Seite **Statistik & Informationen** ist in drei Bereiche unterteilt:

- *Statistiken*
- *Versionen und Aktualisierungen*
- *Berichte*

Statistiken

In diesem Abschnitt werden der Prozentsatz und die Anzahl der sauberen Elemente, der erkannten Spam- und Phishing-Nachrichten, der Viren, der gesperrten Datentypen/Nachrichten und der Nachrichten mit unerwünschtem Inhalt angezeigt. Ferner werden die durchschnittliche Scanzeit (in Millisekunden) und die Gesamtanzahl der gescannten E-Mails eingeblendet.

Klicken Sie auf **Zurücksetzen**, um die Statistiken der erkannten Elemente zurückzusetzen. Wählen Sie im Dropdown-Menü **Diagramm** eine der folgenden Optionen aus:

- **<Erkennungen auswählen>** – Wählen Sie die Zähler im Abschnitt **Erkennungen** aus, indem Sie auf das Symbol eines Elements klicken. So können Sie die Statistiken und das Diagramm der ausgewählten Zähler anzeigen.
- **Spamzusammenfassung** — Zeigen Sie Spamstatistiken und das Diagramm an.
- **Phishingzusammenfassung** — Zeigen Sie Phishingstatistiken und das Diagramm an.

Klicken Sie auf das Symbol **Balkendiagramm anzeigen** oder auf das Symbol **Kreisdiagramm anzeigen** , um die Erkennungen grafisch anzuzeigen. Sie können ebenfalls aus dem Dropdown-Menü die Option **Zeitbereich** auswählen, um diese Diagramme anzuzeigen. Für den Zeitbereich stehen folgende Optionen zur Verfügung:

- **Letzte 24 Stunden**
- **Letzte 7 Tage**
- **Letzte 30 Tage**

Versionen & Aktualisierungen

Dieser Bereich besteht aus drei Registerkarten:

- **Aktualisierungsinformationen**: Auf dieser Registerkarte werden der Zeitpunkt der letzten Aktualisierung der Anti-Virus-Engine und die DAT-Dateien angezeigt. Die Aktualisierungsfrequenz wird ebenfalls angezeigt. Ferner werden die Version des Antivirenmoduls, der DAT-Dateien und des Anti-Spam-Moduls angegeben (wenn Sie das Add-On Anti-Spam für GroupShield installiert haben). Zudem können Sie den Status der letzten Aktualisierung (über den Link **Status anzeigen**) anzeigen und eine neue Aktualisierungsfrequenz (über den Link **Plan bearbeiten**) zeitlich planen.

  McAfee Security veröffentlicht regelmäßig Virusdefinitionsdateien (DAT-Dateien), um die neuesten Viren zu erkennen und zu entfernen. Klicken Sie auf **Jetzt aktualisieren**, um Ihren Antivirus-Schutz auf den neuesten Stand zu bringen.

- **Produktinformationen**: Auf dieser Registerkarte werden der Produktname und die -version, das Service Pack, HotFix-Informationen sowie der Zustand des Schutzes vor Pufferüberläufen angezeigt.

  Bei einem Pufferüberlauf handelt es sich um einen abnormen Zustand, in dem ein Prozess versucht, Daten jenseits der Grenzen eines Puffers mit fester Länge zu speichern. Dies führt dazu, dass Daten in angrenzenden Speicherorten durch weitere Daten überschrieben werden. Durch Aktivieren der Option **Schutz vor Pufferüberläufen** wird dieser Zustand verhindert.

- **Lizenzen**: Auf dieser Registerkarte werden die Beschreibung des installierten Produkts bzw. der installierten Produkte, der Lizenztyp und die Lizenzbeschreibung, das Ablaufdatum (falls es sich um einen Beta-Lizenztyp handelt) und die Anzahl der Tage bis zum Ablauf der Lizenz angezeigt.

Berichte

Dieser Bereich besteht aus drei Registerkarten:

Zuletzt gescannte Elemente: Auf dieser Registerkarte wird eine Liste der zuletzt gescannten Elemente angezeigt. Sie enthält ferner Datum und Uhrzeit des Scans, Details zu Absender und Empfänger, die nach dem Scan durchgeführte Aktion, den Namen des gescannten Dokuments, den Namen der Erkennung, den Typ des Scantasks, den Grund für die Erkennung des Elements sowie den ausgewählten Richtliniennamen.

Antivirus-Nachrichten: Diese Registerkarte enthält eine Liste der Überschriften mit den aktuellen Antivirus-Nachrichten, die ein Unternehmen an einem bestimmten Datum veröffentlicht hat. Hiermit soll auf die aktuellen Virusbedrohungen und Schwachstellen hingewiesen werden. Klicken Sie auf den Link einer Überschrift, um die entsprechenden Nachrichten auf einer Webseite zu lesen.

Sicherheitsnachrichten: Diese Registerkarte enthält eine Liste der an einem bestimmten Datum veröffentlichten Überschriften, die die aktuellen Informationen zur IT-Sicherheit enthalten. Klicken Sie auf den Link einer Überschrift, um die entsprechenden Sicherheitsinformationen auf einer Webseite anzuzeigen.

Scans auf Anforderung

Der Scan auf Anforderung ist eine Methode, mit der E-Mails zu günstigen Zeiten oder in regelmäßigen Intervallen gescannt werden können. Sie können regelmäßige Scanvorgänge planen, wenn diese Ihre Arbeit nicht beeinträchtigen und die Serveraktivitäten vergleichsweise gering sind.

GroupShield für Exchange ermöglicht Ihnen ebenfalls das Erstellen geplanter Scans auf Anforderung. Jeder Plan wird automatisch in vorab festgelegten Intervallen oder zu bestimmten Zeiten ausgeführt.

Im Folgenden werden mögliche Gründe für das Durchführen eines Scans auf Anforderung aufgeführt:

- Um eine bestimmten Datei oder bestimmter Dateien zu prüfen, die geladen oder publiziert wurden.
- Um die Dokumente auf dem Exchange-Server auf Viren zu überprüfen; möglicherweise nach einer DAT-Aktualisierung, wenn neue Viren erkannt werden können.
- Wenn Sie einen Virus, Spam oder eine Phishing-Nachricht erkannt und entfernt haben und prüfen möchten, ob Ihr Computer sauber ist.

Planen eines neuen Scans auf Anforderung

1 Klicken Sie auf **Dashboard** | **Scans auf Anforderung**. Die Seite **Scans auf Anforderung** wird angezeigt.

2 Klicken Sie auf **Neuer Scan**. Die Seite zum Planen eines Scans auf Anforderung wird angezeigt.

3 Wählen Sie unter **Wählen Sie den Zeitpunkt des Scans** eine der folgenden Optionen aus:

- **Nicht geplant** — Aktivieren Sie dieses Kontrollkästchen, und geben Sie die Stunden und Minuten ein, nach denen der Scanvorgang beendet werden soll.
- **Einmalig** — Wählen Sie in den entsprechenden Dropdown-Listen ein Datum, einen Monat, ein Jahr und eine Uhrzeit für den Start eines Scans aus. Sie können das Kontrollkästchen aktivieren und die Stunden und Minuten eingeben, nach denen der Berichtstask beendet werden soll.
- **Stunden** — Mit dieser Option geben Sie an, in welchem Stundenrhythmus der Scanvorgang gestartet wird. Sie können den Zeitpunkt des Scanstarts dabei minutengenau bestimmen. Sie können das Kontrollkästchen aktivieren und die Stunden und Minuten eingeben, nach denen der Berichtstask beendet werden soll.
- **Tage** — Mit dieser Option geben Sie an, in welchem Tagerhythmus der Task gestartet wird. Sie können genau bestimmen, zu welcher Uhrzeit der Task erfolgen soll. Sie können das Kontrollkästchen aktivieren und die Stunden und Minuten eingeben, nach denen der Berichtstask beendet werden soll.
- **Wochen** — Mit dieser Option geben Sie an, in welchem Wochenrhythmus der Task gestartet wird. Sie können auch angeben, an welchem Tag und zu welcher Uhrzeit der Task durchgeführt werden soll. Sie können das Kontrollkästchen aktivieren und die Stunden und Minuten eingeben, nach denen der Berichtstask beendet werden soll.
- **Monate** — Aktivieren Sie entweder für den ersten, zweiten, dritten, vierten oder letzten Tag ein Kontrollkästchen, indem Sie auf den gewünschten Monat klicken und die Uhrzeit für das Starten des Scanvorgangs festlegen.
  Sie können das Kontrollkästchen aktivieren und die Stunden und Minuten eingeben, nach denen der Berichtstask beendet werden soll.

4 Klicken Sie auf **Weiter**. Wählen Sie auf der Seite **Legen Sie fest, was gescannt werden soll**, die gewünschten Ordner aus, und klicken Sie auf >>, um die Ordner aus der Liste **Verfügbare Ordner** in die Liste **Zu scannende Ordner** zu verschieben.

Klicken Sie auf >>>, um einen Ordner und alle zugehörigen Unterordner auszuwählen.

5 Wählen Sie eine der folgenden Optionen aus:

- **Alle Ordner scannen** — Alle Ordner unter **Zu scannende Ordner** werden gescannt.
- **Ausgewählte Ordner scannen** — Unter **Zu scannende Ordner** ausgewählte Ordner werden gescannt.
- **Alle bis auf die folgenden Ordner scannen** — Alle bis auf die unter **Zu scannende Ordner** ausgewählten Ordner werden gescannt.

6 Klicken Sie auf **Weiter** Wählen Sie auf der Seite **Scaneinstellungen konfigurieren**in der Dropdown-Liste die zu verwendende Richtlinie aus. Folgende Optionen stehen zur Verfügung:

- **Auf Anforderung**
- **Viren suchen**
- **Viren entfernen**
- **Gesperrten Inhalt suchen**
- **Gesperrte Inhalte entfernen**
- **Vollständiger Scan**

7 Wählen Sie **Wieder aufnehmbares Scanning**, um **Von letztem Element neu starten** zu aktivieren.

Mit dieser Option können Sie angeben, ob ein Scan an dem Punkt wieder gestartet werden kann, an dem er angehalten wurde.

8 Klicken Sie auf **Weiter**.

9 **Geben Sie einen Namen für den Scantask ein**.

10 Klicken Sie auf **Fertig stellen** und dann auf **Übernehmen**.

Ändern eines vorhandenen Scans auf Anforderung

1 Klicken Sie auf **Dashboard** | **Scans auf Anforderung**. Auf der Seite **Scans auf Anforderung** werden alle Scans auf Anforderung aufgelistet.

2 Klicken Sie auf den Link **Ändern** des zu ändernden Scantasks.

3 Nehmen Sie unter **Wählen Sie den Zeitpunkt des Scans** die erforderlichen Änderungen vor. Klicken Sie auf **Weiter**.

4 Wählen Sie die gewünschten Ordner aus, indem Sie sie nach **Zu scannende Ordner verschieben**. Klicken Sie auf **Weiter**.

5 Wählen Sie in der Dropdown-Liste die gewünschte Richtlinie aus, und geben Sie an, ob der Scan ab dem letzten Element fortgesetzt werden soll. Klicken Sie auf **Weiter**.

6 Geben Sie einen neuen Namen für den Task ein.

7 Klicken Sie auf **Fertig stellen** und dann auf **Übernehmen**.

Löschen eines Scans auf Anforderung

1 Klicken Sie auf **Dashboard** | **Scans auf Anforderung**. Auf der Seite **Scans auf Anforderung** werden alle Scans auf Anforderung aufgelistet.

2 Klicken Sie auf den Link **Löschen** des gewünschten Scantasks.

Der Status des gelöschten Tasks ändert sich in **Für den Löschvorgang markiert**. Klicken Sie auf **Löschen rückgängig machen**, wenn Sie den Task löschen möchten.

3 Klicken Sie auf **Übernehmen**.

Link „Jetzt ausführen“

Sobald Sie einen neuen Task geplant haben, könne Sie einen Scan ausführen.

Diese Option steht nur zur Verfügung, wenn Sie nach dem Erstellen eines neuen Scantasks auf **Übernehmen** klicken.

1 Klicken Sie auf **Dashboard** | **Scans auf Anforderung**. Auf der Seite **Scans auf Anforderung** werden alle Scans auf Anforderung aufgelistet.

2 Klicken Sie für den zu startenden Task auf den Link **Jetzt ausführen**.
Ein Bestätigungsdialogfeld wird angezeigt.

3 Klicken Sie zur sofortigen Ausführung des Scans auf Anforderung auf **OK**.

Klicken Sie auf **Aktualisieren**, um die Zeitplan-Übersichtsinformationen zu aktualisieren.

Statusbericht

Bei einem Statusbericht handelt es sich um einen geplanten Bericht, der zu einem bestimmten Zeitpunkt an den Administrator gesendet wird. Der Bericht enthält Erkennungsstatistiken innerhalb des angegebenen Zeitraums. Sie können eine Uhrzeit, die Empfänger-E-Mail-Adresse/Verteilerliste, an die der Bericht gesendet werden soll, sowie einen Betreff für die E-Mail auswählen. Berichte werden im HTML-Format gesendet.

Planen eines neuen Statusberichts

1 Klicken Sie auf **Dashboard** |**Statusbericht**. Die Seite **Statusbericht** wird angezeigt.

2 Klicken Sie auf **Neuer Bericht**. Die Berichtsseite wird geöffnet.

3 Wählen Sie auf der Seite **Wann ist zu berichten** eine der folgenden Optionen aus:

- **Nicht geplant** — Aktivieren Sie das Kontrollkästchen, um einen Berichtstask einzurichten, der später aktiviert werden kann. Wenn Sie einen Berichtsplan ändern, können Sie mit dieser Option einen vorhandenen Berichtstask stoppen.
- **Einmalig** — Wählen Sie in den entsprechenden Dropdown-Listen ein Datum, einen Monat, ein Jahr und eine Uhrzeit für den Start eines Berichtstasks aus. Sie können das Kontrollkästchen aktivieren und die Stunden und Minuten eingeben, nach denen der Berichtstask beendet werden soll.
- **Stunden** — Mit dieser Option geben Sie an, in welchem Stundenrhythmus der Berichtstask gestartet wird. Sie können den Zeitpunkt des Berichtstasks dabei minutengenau bestimmen. Sie können das Kontrollkästchen aktivieren und die Stunden und Minuten eingeben, nach denen der Berichtstask beendet werden soll.
- **Tage** — Mit dieser Option geben Sie an, in welchem Tagerhythmus der Berichtstask gestartet wird. Sie können genau bestimmen, zu welcher Uhrzeit der Task erfolgen soll. Sie können das Kontrollkästchen aktivieren und die Stunden und Minuten eingeben, nach denen der Berichtstask beendet werden soll.
- **Wochen** — Mit dieser Option geben Sie an, in welchem Wochenrhythmus der Berichtstask gestartet wird. Sie können auch angeben, an welchem Tag und zu welcher Uhrzeit der Task durchgeführt werden soll. Sie können das Kontrollkästchen aktivieren und die Stunden und Minuten eingeben, nach denen der Berichtstask beendet werden soll.
- **Monate** — Aktivieren Sie entweder für den ersten, zweiten, dritten, vierten oder letzten Tag ein Kontrollkästchen, indem Sie auf den gewünschten Monat klicken und die Uhrzeit für das Starten des Berichtstasks festlegen.
  Sie können das Kontrollkästchen aktivieren und die Stunden und Minuten eingeben, nach denen der Berichtstask beendet werden soll.

4 Klicken Sie auf **Weiter**. Die Seite **An wen ist zu berichten** wird angezeigt.

5 Unter **Empfänger-E-Mail** geben Sie die E-Mail-Adresse des Empfängers an, an den der Bericht gesendet werden soll.

6 Unter **Betreffzeile für Bericht** die Betreffzeile für den Bericht ein, der an den Empfänger gesendet wird.

7 Klicken Sie auf **Weiter**. Die Seite **Geben Sie einen Tasknamen ein** wird angezeigt.

8 Geben Sie einen sinnvollen Namen für den Task ein.

9 Klicken Sie auf **Fertig stellen**.

Klicken Sie auf den Link **Ändern** eines Berichtstasks, um seine Einstellungen zu ändern, oder klicken Sie auf den Link **Löschen** eines Berichtstask, um ihn zu löschen.

Link „Jetzt ausführen“

Sobald Sie einen neuen Task geplant haben, könne Sie einen Berichtstask ausführen.

Diese Option steht nur zur Verfügung, wenn Sie nach dem Erstellen eines neuen Berichtstasks auf **Übernehmen** klicken.

1 Klicken Sie auf **Dashboard |Statusbericht**. In der Seite **Statusbericht** werden alle Berichtstasks aufgeführt.

2 Klicken Sie für den zu startenden Task auf den Link **Jetzt ausführen**.
Ein Bestätigungsdialogfeld wird angezeigt.

3 Klicken Sie auf **OK**.

Klicken Sie auf **Aktualisieren**, um die Zeitplan-Übersichtsinformationen zu aktualisieren.

Graphische Berichte

Unter **Grafische Berichte** wird ein Diagramm mit erkannten Elementen im Detail angezeigt. Sie können ebenfalls jede einzelne Erkennung anzeigen, indem Sie Filter zur Anzeige des gewünschten Erkennungstyps festlegen.

Auf der Seite **Grafische Berichte** werden zwei Registerkarten angezeigt:

- **Einfach**
- **Erweitert**

Einfache Berichte

Anzeigen einfacher graphischer Berichte:

1 Klicken Sie auf **Dashboard** | **Grafische Berichte**. Die Seite **Grafische Berichte** wird standardmäßig mit der Registerkarte **Einfach** angezeigt.

2 Wählen Sie unter **Zeitbereich** die Option **Heute** oder **Diese Woche** aus, um nur die Erkennungen des aktuellen Tages oder der letzten 7 Kalendertage (einschließlich des aktuellen Tages) anzuzeigen.

3 Wählen Sie unter **Filter** eine der folgenden Optionen aus:
Top 10-Viren, **Top 10-Spamerkennungen, Top 10-Spamempfänger, Top 10-Phishingerkennungen, Top 10-Unerwünschte Programme**, **Top 10-Erkennungen unerwünschter Inhalte**, **Top 10-Infizierte Dateien** oder **Erkennungen**.

4 Klicken Sie auf **Suchen**.

Erweiterte Berichte

Unter **Erweiterte Berichte** können Sie Filter setzen, um die Suchkriterien einzuschränken.

Anzeigen eines erweiterten Berichts mit Suchfiltern:

1 Klicken Sie auf **Dashboard** | **Grafische Berichte**. Die Seite **Grafische Berichte** wird geöffnet.

2 Klicken Sie auf die Registerkarte **Erweitert**.

3 Wählen Sie mindestens einen und höchstens drei der folgenden Filter aus:

- **Betreff**
- **Empfänger**
- **Grund**
- **Ticketnummer**

- **Erkennungsname**
- **Spamfaktor**

4 Wählen Sie **Alle Datumsangaben** oder den gewünschten **Datumsbereich** in den Dropdown-Listen aus.

5 Wählen Sie **Balkendiagramm** oder **Kreisdiagramm** aus.

6 Bei Auswahl von **Kreisdiagramm** wählen Sie in der Dropdown-Liste **Abfrage für** aus.

- **Empfänger**
- **Absender**
- **Dateiname**
- **Erkennungsname**
- **Betreff**
- **Grund**
- **Regelname**
- **Richtlinienname**
- **Spamfaktor**

7 Geben Sie im Feld **Maximale Anzahl Ergebnisse** die maximale Anzahl der Segmente an, die im Kreisdiagramm angezeigt werden sollen.
Wenn Sie beispielsweise lediglich die drei am häufigsten zugewiesenen Spamfaktoren anzeigen möchten, geben Sie 3 ein.

Abfrage für und **Maximale Anzahl Ergebnisse** sind nur für das Kreisdiagramm verfügbar.

8 Klicken Sie auf **Suchen**.

Klicken Sie auf **Filter löschen**, um zu den Standardfilterwerten zu wechseln.

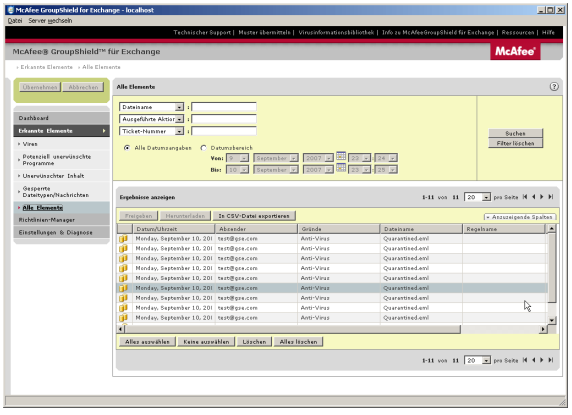
9 Erkannte Elemente

Unter **Erkannte Elemente** werden Informationen zu E-Mails angezeigt, die Spam, Phishing, Viren, potenziell unerwünschte Programme, unerwünschten Inhalt, gesperrte Dateitypen oder Nachrichten sowie alle Elemente enthalten. Sie sollten mindestens einen Suchfilter auswählen, Sie können aber auch bis zu drei Suchfilter zur Eingrenzung Ihrer Suche verwenden.

Folgende Themen werden behandelt:

- **Spam**
- **Phishing**
- **Viren**
- **Potenziell unerwünschte Programme**
- **Unerwünschter Inhalt**
- **Gesperrte Dateitypen/Nachrichten**
- **Alle Elemente**

Abbildung 9-1 Erkannte Elemente



Spam

Bei Spam handelt es sich um unerwünschte E-Mails, insbesondere unerwünschte Massensendungen.

1 Klicken Sie auf **Erkannte Elemente | Spam**. Die Seite **Spam** wird angezeigt.

2 Wählen Sie bis zu drei der folgenden Suchfilter aus:

- **Ticketnummer**
- **Absender**
- **Spamfaktor**
- **Ausgeführte Aktion**

3 Wählen Sie **Alle Datumsangaben**, um alle Einträge aufzunehmen. Alternativ können Sie das gewünschte Datum und den gewünschten Zeitraum in den Dropdown-Listen unter **Datumsbereich** auswählen.

4 Klicken Sie auf **Suchen**. Im Abschnitt **Ergebnisse anzeigen** wird eine Liste der Spamelemente angezeigt, die Ihren Suchkriterien entsprechen.

Klicken Sie auf **Filter löschen**, um zu den Standardeinstellungen für Suchfilter zurückzukehren.

Phishing

Bei Phishing handelt es sich um eine Methode, mit der Betrüger versuchen, sich persönliche Daten wie Kennwörter, Sozialversicherungsnummern oder Kreditkartendaten anzueignen, indem sie gefälschte E-Mails versenden, die echten E-Mails von vertrauenswürdigen Unternehmen oder Banken täuschend ähnlich sehen.

In der Regel werden die Empfänger von Phishing-E-Mails dazu aufgefordert, auf einen Link in der E-Mail zu klicken, um ihre Kontakt- oder Kreditkartendaten zu prüfen, bestätigen oder aktualisieren.

1 Klicken Sie auf **Erkannte Elemente** | **Phishing**. Die Seite **Phishing** wird angezeigt.

2 Wählen Sie bis zu drei der folgenden Suchfilter aus:

- **Ticketnummer**
- **Absender**
- **Spamfaktor**
- **Ausgeführte Aktion**

3 Wählen Sie **Alle Datumsangaben**, um alle Einträge aufzunehmen. Alternativ können Sie das gewünschte Datum und den gewünschten Zeitraum in den Dropdown-Listen unter **Datumsbereich** auswählen.

4 Klicken Sie auf **Suchen**. Im Abschnitt **Ergebnisse anzeigen** wird eine Liste der Phishingelemente angezeigt, die Ihren Suchkriterien entsprechen.

Klicken Sie auf **Filter löschen**, um zu den Standardeinstellungen für Suchfilter zurückzukehren.

Viren

Ein Virus ist ein Programm oder Code, der sich selbst repliziert, multipliziert und ein anderes sinnvolles Programm, den Bootsektor, den Partitionssektor oder Makros unterstützende Dokumente infiziert, indem er sich in das Medium einfügt oder daran anhängt. Die meisten Viren replizieren sich, und viele beschädigen das System erheblich.

1 Klicken Sie auf **Erkannte Elemente** | **Viren**. Die Seite **Viruserkennungen** wird angezeigt.

2 Wählen Sie bis zu drei der folgenden Suchfilter aus:

- **Ticketnummer**
- **Dateiname**
- **Ausgeführte Aktion**
- **An AVERT übermitteln**

3 Wählen Sie **Alle Datumsangaben**, um alle Einträge aufzunehmen. Alternativ können Sie das gewünschte Datum und den gewünschten Zeitraum in den Dropdown-Listen unter **Datumsbereich** auswählen.

4 Klicken Sie auf **Suchen**. Im Abschnitt **Ergebnisse anzeigen** wird eine Liste der Viren angezeigt, die Ihren Suchkriterien entsprechen.

Klicken Sie auf **Filter löschen**, um zu den Standardeinstellungen für Suchfilter zurückzukehren.

Potenziell unerwünschte Programme

Potenziell unerwünschte Programme (PUPs) sind von legitimen Unternehmen geschriebene Softwareprogramme, die im Fall der Installation den Sicherheits- oder Vertraulichkeitsstatus des Computers verändern können.

1 Klicken Sie auf **Erkannte Elemente** | **Potenziell unerwünschte Programme**. Die Seite **Potenziell unerwünschte Programme** wird angezeigt.

2 Wählen Sie bis zu drei der folgenden Suchfilter aus:

- **Ticketnummer**
- **Dateiname**
- **Ausgeführte Aktion**
- **An AVERT übermitteln**

3 Wählen Sie **Alle Datumsangaben**, um alle Einträge aufzunehmen. Alternativ können Sie das gewünschte Datum und den gewünschten Zeitraum in den Dropdown-Listen unter **Datumsbereich** auswählen.

4 Klicken Sie auf **Suchen**. Im Abschnitt **Ergebnisse anzeigen** wird eine Liste der potenziell unerwünschten Programme angezeigt, die Ihren Suchkriterien entsprechen.

Klicken Sie auf **Filter löschen**, um zu den Standardeinstellungen für Suchfilter zurückzukehren.

Unerwünschter Inhalt

Alle vom Scanner gefilterten Inhalte werden als „Unerwünschter Inhalt“ bezeichnet. Verwenden Sie **Unerwünschter Inhalt**, um E-Mails/Anhänge mit unerwünschtem Inhalt anzuzeigen.

1 Klicken Sie auf **Erkannte Elemente | Unerwünschter Inhalt**. Die Seite **Unerwünschter Inhalt** wird angezeigt.

2 Wählen Sie einen der folgenden Suchfilter aus:

- **Ticketnummer**
- **Dateiname**
- **Ausgeführte Aktion**

3 Wählen Sie **Alle Datumsangaben**, um alle Einträge aufzunehmen. Alternativ können Sie das gewünschte Datum und den gewünschten Zeitraum in den Dropdown-Listen unter **Datumsbereich** auswählen.

4 Klicken Sie auf **Suchen**. Im Abschnitt **Ergebnisse anzeigen** wird eine Liste der Dateien mit unerwünschtem Inhalt angezeigt, die Ihren Suchkriterien entsprechen.

Klicken Sie auf **Filter löschen**, um zu den Standardeinstellungen für Suchfilter zurückzukehren.

Gesperrte Dateitypen/Nachrichten

Als „Gesperrte Dateitypen“ werden alle von einem Netzwerkadministrator gesperrten Dateien bezeichnet.

1 Klicken Sie auf **Erkannte Elemente** | **Gesperrte Dateitypen/Nachrichten**.

2 Wählen Sie einen der folgenden Suchfilter aus:

- **Ticketnummer**
- **Dateiname**
- **Ausgeführte Aktion**

3 Wählen Sie **Alle Datumsangaben**, um alle Einträge aufzunehmen. Alternativ können Sie das gewünschte Datum und den gewünschten Zeitraum in den Dropdown-Listen unter **Datumsbereich** auswählen.

4 Klicken Sie auf **Suchen**. Im Abschnitt **Ergebnisse anzeigen** wird eine Liste der gesperrten Dateitypen/Nachrichten angezeigt, die Ihren Suchkriterien entsprechen.

Klicken Sie auf **Filter löschen**, um zu den Standardeinstellungen für Suchfilter zurückzukehren.

Alle Elemente

Verwenden Sie **Alle Elemente**, um alle E-Mails anzuzeigen, die erkannte Elemente enthalten.

1 Klicken Sie auf **Erkannte Elemente** | **Alle Elemente**. Die Seite **Alle Elemente** wird angezeigt.

2 Wählen Sie einen der folgenden Suchfilter aus:

- **Ticketnummer**
- **Dateiname**
- **Ausgeführte Aktion**

3 Wählen Sie **Alle Datumsangaben**, um alle Einträge aufzunehmen. Alternativ können Sie das gewünschte Datum und den gewünschten Zeitraum in den Dropdown-Listen unter **Datumsbereich** auswählen.

4 Klicken Sie auf **Suchen**. Im Abschnitt **Ergebnisse anzeigen** wird eine Liste der gesperrten Dateitypen/Nachrichten angezeigt, die Ihren Suchkriterien entsprechen.

Klicken Sie auf **Filter löschen**, um zu den Standardeinstellungen für Suchfilter zurückzukehren.

Verwendete Suchfilter:

- **Ausgeführte Aktion** — Als Suchkriterium dient die Aktion, die bei Erkennung des Elements ausgeführt wurde.
- **Dateiname** — Als Suchkriterium dient der Dateiname.
- **Absender** — Als Suchkriterium dient die E-Mail-Adresse des Absenders.
- **Spamfaktor** — Als Suchkriterium dient der Spamfaktor. Der Spamfaktor ist eine Zahl, die den Anteil an potenziellem Spam in einer E-Mail angibt.
- **Ticketnummer** — Als Suchkriterium dient die Ticketnummer. Bei einer Ticketnummer handelt es sich um einen 16-stelligen alphanumerischen Eintrag, der von GroupShield für jede Erkennung automatisch generiert wird. Die Ticketnummer kann in die Benachrichtigungs-E-Mail aufgenommen werden. Standardmäßig enthalten Benachrichtigungs-E-Mails keine Ticketnummer.

Aufnehmen einer Ticketnummer in eine Benachrichtigungs-E-Mail:

1. Klicken Sie unter **Einstellungen & Diagnose** auf **Benachrichtigungen**. Die Seite **Benachrichtigungen** wird angezeigt.
2. Klicken Sie auf **Bearbeiten**. Das Dialogfeld **GroupShield für Exchange - Benachrichtigungstext** wird angezeigt.
3. Fügen Sie **Ticketnummer: %tik%** hinzu.
4. Klicken Sie auf **Speichern** und dann auf **Übernehmen**.

Der Bereich „Ergebnisse anzeigen“

Folgende Aufgaben können Sie aus dem Abschnitt **Ergebnisse anzeigen** aller erkannten Elemente ausführen:

- Freigeben eines isolierten Elements. Wählen Sie im Bereich **Ergebnisse anzeigen** einen Datensatz aus, und klicken Sie auf **Freigeben**. Die Original-E-Mail wird aus der Datenbank freigegeben und dem eigentlichen Empfänger zugestellt.
- Herunterladen einer isolierten E-Mail. Wählen Sie im Bereich **Ergebnisse anzeigen** einen Datensatz aus, und klicken Sie auf **Herunterladen**.
- Exportieren und Speichern von Einträgen im CSV-Format. Wählen Sie im Bereich **Ergebnisse anzeigen** einen Datensatz aus, und klicken Sie auf **In CSV-Datei exportieren**.
- Übermitteln eines isolierten Elements an AVERT. Wählen Sie im Bereich **Ergebnisse anzeigen** einen Datensatz aus, und klicken Sie auf **An AVERT übermitteln**.

Des Weiteren stehen folgende Optionen zur Verfügung:

- **Anzuzeigende Spalten** — Weitere Spaltenköpfe für den Bereich **Ergebnisse anzeigen** können ausgewählt werden. Klicken Sie auf diese Option, wählen Sie die gewünschten Optionen aus, und klicken Sie auf **OK**.

  Sie müssen mindestens einen Spaltenkopf auswählen.

- **Alles auswählen** — Alle erkannten Elemente im Bereich **Ergebnisse anzeigen** werden ausgewählt.
- **Keine auswählen** — Die Auswahl aller erkannten Elemente im Bereich **Ergebnisse anzeigen** wird aufgehoben.
- **Löschen** — Die ausgewählten erkannten Elemente im Bereich **Ergebnisse anzeigen** werden gelöscht.
- **Alles löschen** — Alle erkannten Elemente im Bereich **Ergebnisse anzeigen** werden gelöscht.

10 Richtlinien-Manager

In diesem Kapitel wird die Durchsetzung von Richtlinien in GroupShield für Microsoft® Exchange Server 2003/2007 erläutert. Mit dem **Richtlinien-Manager** können Sie Richtlinien zur Handhabung unterschiedlicher Bedrohungen angeben.

Für jeden Richtlinientyp gibt es eine Masterrichtlinie, bei der es sich um die Standardrichtlinien für diesen Richtlinientyp handelt. Ein Löschen der Masterrichtlinie ist nicht möglich, da es immer eine Richtlinie geben sollte, die als Basis für das Erstellen anderer Richtlinien dient. Die Masterrichtlinie sollte so konfiguriert sein, dass sie für die meisten Situationen anwendbar ist. Für Ausnahmesituationen, die nicht von der Masterrichtlinie abgefangen werden, können Sie Unterrichtlinien erstellen.

Sie können die Reihenfolge festlegen, in der Unterrichtlinien angewendet werden. Unterrichtlinien haben gegenüber der Masterrichtlinie Priorität.

Ansichten im Richtlinien-Manager

Im Richtlinien-Manager stehen zwei Ansichten zur Verfügung:

- **Vererbungsansicht**
- **Erweiterte Ansicht**

Vererbungsansicht

In der **Vererbungsansicht** können Sie Richtlinieneinstellungen anzeigen, die von einer anderen Richtlinie geerbt wurden.

Eine Richtlinie, die ihre Einstellungen geerbt hat, wird als untergeordnete Richtlinie bezeichnet, wohingegen eine Richtlinie, die ihre Einstellungen vererbt, eine übergeordnete Richtlinie ist. Wenn der Name einer Richtlinie eingerückt ist, bedeutet dies, dass diese Richtlinie einige Einstellungen von einer übergeordneten Richtlinie erbt.

Sie haben folgende Möglichkeiten:

- **Name** der Richtlinie — Wird zum Bearbeiten der Richtlinieneinstellungen verwendet.
- Spalte **Priorität** — Zeigt die Reihenfolge an, in der die Richtlinien angewendet werden.
- **Unterrichtlinie erstellen** — Erstellt eine Unterrichtlinie.
- Link **Löschen** — Löscht eine Unterrichtlinie, die nicht mehr erforderlich ist.
- **Aktiviert** — Aktiviert oder deaktiviert eine Unterrichtlinie. Wenn Sie diese Option auswählen, wird die Unterrichtlinie aktiviert.
- **Übernehmen** — Übernimmt die vorgenommenen Einstellungen/Änderungen.

Erweiterte Ansicht

Unter **Erweiterter Ansicht** haben Sie vor allem die Möglichkeit, die Reihenfolge zu ändern, in der Unterrichtlinien angewendet werden (Spalte **Verschieben**).

Sie haben folgende Möglichkeiten:

- **Name** der Richtlinie — Wird zum Bearbeiten der Richtlinieneinstellungen verwendet.
- **Unterrichtlinie erstellen** — Erstellt eine Unterrichtlinie.

Sie können eine Unterrichtlinie für Ausnahmen erstellen, die nicht von der Masterrichtlinie abgedeckt sind.

- **Aktiviert** — Aktiviert oder deaktiviert eine Unterrichtlinie. Wenn Sie diese Option auswählen, wird die Unterrichtlinie aktiviert.
- Link **Löschen** — Löscht eine Unterrichtlinie, die nicht mehr erforderlich ist.
- Link **Details** — Zeigt die Beschreibung der Richtlinie und die Abstammung an.
- **Übernehmen** — Übernimmt die vorgenommenen Einstellungen/Änderungen.

Erstellen einer Unterrichtlinie

1 Wählen Sie unter **Richtlinien-Manager** ein Menüelement aus, für das Sie eine Unterrichtlinie erstellen möchten.

2 Klicken Sie auf **Unterrichtlinie erstellen.** Die Seite **Unterrichtlinie erstellen** wird mit drei Registerkarten angezeigt:

- **Anfangskonfiguration**
- **Auslöseregeln**
- **Scanner und Filter**

3 Geben Sie auf der Seite **Anfangskonfiguration** unter **Name der Unterrichtlinie** einen Richtliniennamen ein, der die Richtlinie und ihren Zweck kennzeichnet.

4 Geben Sie eine **Beschreibung** für die Richtlinie ein, wählen Sie im Dropdown-Menü eine übergeordnete Richtlinie für die Unterrichtlinie aus, und klicken Sie dann auf **Weiter**. Die Seite **Auslöseregeln** wird angezeigt.

5 Legen Sie die Bedingungen für das Auslösen der Richtlinie fest. Wählen Sie für die einzelnen Benutzer **Eine der Regeln zutrifft**, **Alle Regeln zutreffen** oder **Keine der Regeln zutrifft** aus.

6 Klicken Sie auf **Neue Regel**. Wählen Sie im Abschnitt **Richtlinienregel angeben** eine dieser primären Regeln, und geben Sie eine entsprechende sekundäre Regel an:

- **Die SMTP-Adresse des Absenders ist E-Mail-Adresse**
- **Die SMTP-Adresse des Absenders ist nicht E-Mail-Adresse**
- **Die SMTP-Adresse einer der Empfänger ist E-Mail-Adresse**
- **Die SMTP-Adresse einer der Empfänger ist nicht E-Mail-Adresse**
- **Der Absender befindet sich in Active Directory-Gruppe**
- **Der Absender befindet sich nicht in Active Directory-Gruppe**
- **Einer der Empfänger befindet sich in Active Directory-Gruppe**
- **Einer der Empfänger befindet sich nicht in Active Directory-Gruppe**

7 Klicken Sie auf **Hinzufügen**, um die Auslöseregel auszuwählen.

Wenn die Schritte 9 und 10 nicht ausgeführt werden sollen, können Sie durch Auswahl von **Regeln aus einer anderen Richtlinie kopieren** im Dropdown-Menü Regeln einer anderen Richtlinie kopieren.

8 Klicken Sie auf **Weiter.** Die Seite **Scanner und Filter** wird angezeigt.

9 Wählen Sie auf der Seite **Initialisierung von Scannern und Filtern für Richtlinie** eine der folgenden Optionen aus:

- **Alle Einstellungen werden aus der übergeordneten Richtlinie vererbt** — Es werden alle Eigenschaften der Masterrichtlinie vererbt.
- **Ausgewählte Einstellungen mit Werten initialisieren, die aus einer anderen Richtlinie kopiert wurden** — Es wird in der Dropdown-Liste eine Richtlinie ausgewählt und die ausgewählten Einstellungen werden mit Werten dieser Richtlinie initialisiert.

10 Klicken Sie auf **Fertig stellen** und dann auf **Übernehmen**.

Richtlinieneinstellungen

Sie können Richtlinien festlegen, die die Handhabung verschiedener Arten von Bedrohungen für unterschiedliche, auf dem Server gespeicherte Benutzergruppen oder Datenbanken regeln. In jeder Richtlinie sind die zu verwendenden Einstellungen und Aktionen festgelegt sowie die durchzuführenden Aktionen bei einer Erkennung in der Exchange-Umgebung. Die Einstellungen erhalten Namen und können von mehreren Richtlinien gleichzeitig verwendet werden. Die Aktionen sind jedoch richtlinienspezifisch.

1 Wählen Sie im **Richtlinien-Manager** ein Menüelement aus.

2 Klicken Sie auf eine Richtlinie des gewünschten Untermenüelements, für das Sie Einstellungen und Aktionen konfigurieren möchten. Die Seite Richtlinie wird mit den drei Registerkarten **Alle Scanner auflisten**, **Einstellungen anzeigen** und **Benutzer angeben** angezeigt.

Alle Scanner auflisten

Auf der Registerkarte **Alle Scanner auflisten** können Sie die verschiedenen Richtlinieneinstellungen vornehmen. Die verfügbaren Einstellungstypen sind abhängig vom ausgewählten Scanner bzw. Filter. Sie haben folgende Möglichkeiten:

- **Richtlinie** — Ermöglicht die Auswahl der zu konfigurierenden Richtlinie (in der Dropdown-Liste).

- **Scanner/Filter hinzufügen** — Konfiguriert die Richtlinie so, dass sie nur zu bestimmten Zeiten angewendet wird. Sie können beispielsweise Antivirus-Einstellungen festlegen, die nur an Wochenenden gelten.

  Weitere Informationen zu **Scanner/Filter hinzufügen** finden Sie unter *Hinzufügen von Scannern/Filtern auf Seite 122*.

- **Kernscanner** — Ermöglicht die Konfiguration der Richtlinie für die einzelnen Scannertypen. Zu den standardmäßigen Kernscannern gehören:
  - **Antivirenscanner**
  - **Inhaltsscan**
  - **Dateifilterung**
  - **Anti-Spam (Gateway)**
  - **Anti-Phishing (Gateway)**

  Weitere Informationen zu den oben erwähnten **Kernscannern** finden Sie unter *Scanner und Filter auf Seite 124*

- **Filter** — Konfiguriert die Richtlinie für jeden Filtertyp. Zu den Standardfiltern gehören:
  - **Beschädigter Inhalt**
  - **Geschützter Inhalt**
  - **Verschlüsselter Inhalt**
  - **Signierter Inhalt**
  - **Kennwortgeschützte Dateien**
  - **Scannersteuerung**
  - **Einstellungen für MIME-Nachrichten.**
  - **HTML-Dateien**
  - **Nachrichtengrößenfilterung (Gateway)**

  Weitere Informationen zu den oben erwähnten **Filtern** finden Sie unter *Filter auf Seite 148*.

- **Verschiedenes** — Ermöglicht die Konfiguration von Warnmeldungen für diese Richtlinie. Zu diesen Einstellungen gehören:

- **Warneinstellungen**
- **Text für Haftungsausschluss (Gateway)**

Weitere Informationen zu den Einstellungen unter **Verschiedenes** finden Sie unter *Verschiedenes auf Seite 169*.

Hinzufügen von Scannern/Filtern

1 Wählen Sie unter **Richtlinien-Manager** ein Untermenüelement aus. Die Richtlinienseite für das Untermenüelement wird angezeigt.

2 Wählen Sie die gewünschte Richtlinie aus der Dropdown-Liste aus.

3 Klicken Sie auf **Scanner/Filter hinzufügen**. Die Seite **Zeitlich begrenzte Konfiguration erstellen** wird angezeigt.

4 Wählen Sie die erforderliche Scanner-/Filterkategorie in der Dropdown-Liste aus.

5 Geben Sie unter **Verwendungszeit dieser Instanz** an, ob Sie einen vorhandenen Zeitrahmen verwenden oder einen neuen für diese zeitlich begrenzte Richtlinie erstellen möchten.

6 Wenn Sie **Vorhandenes Zeitintervall auswählen** aktivieren, wählen Sie eine der folgenden Optionen im Dropdown-Menü aus:

- **Wochentage**
- **Wochenenden**
- **Arbeitsstunden**

7 Wenn Sie **Neues Zeitintervall erstellen** auswählen, geben Sie einen Namen für das neue Zeitintervall an, und wählen Sie die entsprechenden Tage und die entsprechende Zeit aus.

8 Klicken Sie auf **Speichern** und dann auf **Übernehmen**.

Sie können ein neues, selbst erstelltes Zeitintervall löschen.

Einstellungen anzeigen

Auf der Registerkarte **Einstellungen anzeigen** können Sie die Scanner-/Filtereinstellungen einer bestimmten Richtlinie sowie den ausgewählten Scanner/Filter konfigurieren. Sie haben folgende Möglichkeiten:

- Anzeigen und Konfigurieren von Optionseinstellungen, einschließlich Festlegen der zu verwendenden Warnmeldung, wenn eine Inhaltsregel von einer Erkennung ausgelöst wird.
- Anzeigen und Konfigurieren von Inhaltsregeln und Aktionen.
- Anzeigen und Konfigurieren der gewünschten Aktion beim Auftreten einer Erkennung.

Auf der Registerkarte **Einstellungen anzeigen** wird eine Zusammenfassung der wichtigsten Einstellungen für die ausgewählte Richtlinie und Scanner/Filter angezeigt. Außerdem können Sie diese Einstellungen hier ändern. Sie können beispielsweise die Richtlinie aktivieren oder deaktivieren und die der Richtlinie zugewiesene Warnmeldung ändern.

Benutzer angeben

Auf der Registerkarte **Benutzer angeben** können Sie angeben, für welche Benutzer welche Richtlinienregeln gelten sollen.

Erstellen einer Regel für einen bestimmten Benutzer

1. Legen Sie im Bereich **Benutzer angeben, für die diese Richtlinie gilt** die Bedingungen fest, bei denen die Richtlinie ausgelöst wird.Wählen Sie für den entsprechenden Benutzer **Eine der Regeln zutrifft**, **Alle Regeln zutreffen** oder **Keine Regel zutrifft** aus.
2. Klicken Sie auf **Neue Regel**.
3. Wählen Sie im Bereich **Richtlinienregel angeben** die Richtlinienregel aus, und definieren Sie die Bedingungen für die Regel. Folgende Regelvorlagen für Richtlinien stehen zur Auswahl:
   - **Die SMTP-Adresse des Absenders ist E-Mail-Adresse**
   - **Die SMTP-Adresse des Absenders ist nicht E-Mail-Adresse**
   - **Die SMTP-Adresse einer der Empfänger ist E-Mail-Adresse**
   - **Die SMTP-Adresse einer der Empfänger ist nicht E-Mail-Adresse**
   - **Der Absender befindet sich in Active Directory-Gruppe**
   - **Der Absender befindet sich nicht in Active Directory-Gruppe**

- **Einer der Empfänger befindet sich in Active Directory-Gruppe**
- **Einer der Empfänger befindet sich nicht in Active Directory-Gruppe**

4 Klicken Sie auf **Hinzufügen**, um die Auslöseregel auszuwählen.

Wenn die Schritte 3 und 4 nicht ausgeführt werden sollen, können Sie durch Auswahl von **Regeln aus einer anderen Richtlinie kopieren** im Dropdown-Menü Regeln einer anderen Richtlinie kopieren.

5 Klicken Sie auf **Übernehmen**.

Scanner und Filter

Der Richtlinienmanager beinhaltet Kernscanner, Filter sowie verschiedene Einstellungen für verschiedene Richtlinientypen (Untermenüelemente).
Die verschiedenen Scantypen in GroupShield für Exchange lauten wie folgt:

- **Bei Zugriff** — Richtlinien für E-Mails werden jedes Mal erstellt, wenn E-Mails geöffnet, kopiert oder gespeichert werden, um festzustellen, ob ein Virus oder anderer unerwünschter Code enthalten ist. Scannen bei Zugriff wird auch als Echtzeitscan bezeichnet.
- **Auf Anforderung (Standard)** — Richtlinien werden erstellt, die in festgelegten Intervallen oder auf Anforderung aktiviert werden, um Viren oder potenziell unerwünschten Code zu finden.
- **Auf Anforderung (Viren suchen)** — Richtlinien werden erstellt, die in festgelegten Intervallen oder auf Anforderung aktiviert werden, um Viren oder potenziell unerwünschte Programme und andere mögliche Bedrohungen zu finden.
- **Auf Anforderung (Viren entfernen)** — Richtlinien werden erstellt, die in festgelegten Intervallen oder auf Anforderung aktiviert werden und die Viren, potenziell unerwünschte Programme und andere mögliche Bedrohungen entfernen.
- **Auf Anforderung (Gesperrte Inhalte suchen)** — Richtlinien werden erstellt, die zu festgelegten Intervallen oder auf Anforderung aktiviert werden, um gesperrten Inhalt, der nicht in E-Mails angezeigt werden soll, zu ermitteln.

- **Auf Anforderung (Gesperrte Inhalte entfernen)** — Richtlinien werden erstellt, die zu festgelegten Intervallen oder auf Anforderung aktiviert werden und von Ihnen unerwünschte Inhalte aus E-Mails entfernen. Beispielsweise können Sie eine Richtlinie definieren, die den Inhalt der E-Mail durch eine Warnung ersetzt, wenn diese E-Mail ein unzulässiges Wort oder einen unzulässigen Ausdruck enthält. Verwenden Sie derartige Richtlinien, um zu vermeiden, dass bestimmte Informationen aus dem Unternehmen oder in das Unternehmen gelangen.
- **Auf Anforderung (Vollständiger Scan)** — Richtlinien werden erstellt, die zu festgelegten Intervallen oder auf Anforderung aktiviert werden.
- **Gateway** — Richtlinien für E-Mails werden jedes Mal erstellt, wenn E-Mails geöffnet, kopiert oder gespeichert werden, um festzustellen, ob es sich um Spam, Phishing, MIME- oder HTML-Dateien handelt.

Im Folgenden werden die Kernscanner, Filter und verschiedenen Einstellungen für jeden Richtlinientyp ausführlich erläutert.

Kernscanner

Folgende Scanner gehören zu den Kernscanner in GroupShield 7.0:

- **Antivirenscanner**
- **Inhaltsscan**
- **Dateifilterung**
- **Anti-Spam**
- **Anti-Phishing**

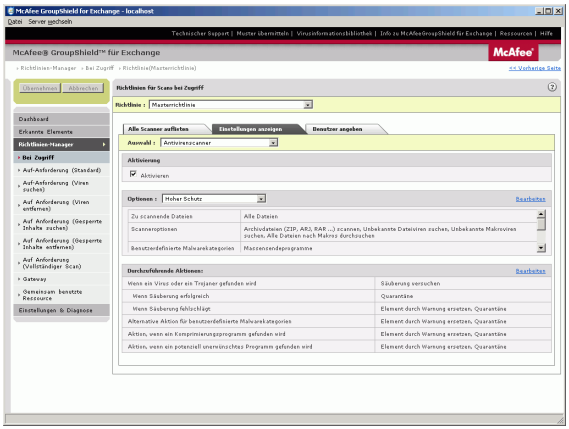
Antivirenscanner

Antivirenscanner ist ein Computerprogramm zum Identifizieren, Verhindern und Löschen von Computerviren und anderer bösartiger Software.

1. Wählen Sie unter **Richtlinien-Manager** ein Untermenüelement aus. Die Richtlinienseite für das Untermenüelement wird angezeigt.
2. Wählen Sie die gewünschte Richtlinie aus dem Dropdown-Menü aus.

3 Klicken Sie auf **Antivirenscanner**. Die Registerkarte **Einstellungen anzeigen** für den Antivirenscanner wird angezeigt.

Abbildung 10-1 Antivirenscanner



4 Aktivieren oder deaktivieren Sie unter **Aktivierung** das Kontrollkästchen **Aktivieren**, um die Einstellungen für den Antivirenscanner für diese Richtlinie ein- oder auszuschalten.

5 Wählen Sie unter **Optionen** die anzuzeigenden oder zu konfigurierenden Virenschutzoptionen aus:

- **Hoher Schutz** — Zum Anzeigen und Konfigurieren der Einstellungen, die angewendet werden, wenn eine hohe Sicherheitsstufe erforderlich ist.
- **Mittlerer Schutz** — Zum Anzeigen und Konfigurieren der Einstellungen, die angewendet werden, wenn eine mittlere Sicherheitsstufe erforderlich ist.
- **Geringer Schutz** — Zum Anzeigen und Konfigurieren der Einstellungen, die angewendet werden, wenn eine geringe Sicherheitsstufe erforderlich ist.
- **neuen Optionssatz erstellen** — Zum Erstellen eines neuen Optionssatzes für diese Richtlinie.

Die schrittweisen Anleitungen zur Verwendung der Option **neuen Optionssatz erstellen** finden Sie unter *Erstellen eines neuen Optionssatzes im Antivirenscanner auf Seite 127*.

6 Klicken Sie zum Bearbeiten des ausgewählten Optionssatzes unter **Optionen** auf den Link **Bearbeiten**.

7 Unter **Durchzuführende Aktionen** können Sie eine Zusammenfassung der in unterschiedlichen Situationen auszuführenden Aktionen anzeigen und bearbeiten. Klicken Sie zum Ändern dieser Aktionen auf **Bearbeiten**.

Informationen zum Bearbeiten der Antivirenscanner-Aktionen finden Sie unter *Bearbeiten von Antivirenscanner-Aktionen auf Seite 130*.

Erstellen eines neuen Optionssatzes im Antivirenscanner

1 Wählen Sie unter **Richtlinien-Manager** ein Untermenüelement aus, das über einen Antivirenscanner verfügt. Die Richtlinienseite für das Untermenüelement wird angezeigt.

2 Wählen Sie die gewünschte Richtlinie aus der Dropdown-Liste aus.

3 Klicken Sie auf **Antivirenscanner**. Die Registerkarte **Einstellungen anzeigen** für den Antivirenscanner wird angezeigt.

4 Klicken Sie im Dropdown-Menü **Optionen** auf **neuen Optionssatz erstellen**. Die Seite **Antivirus-Scannereinstellungen** wird mit vier Registerkarten angezeigt:

- **Grundlegende Optionen**
- **Erweitert**
- **Komprimierungsprogramme**
- **Potenziell unerwünschte Programme**

5 Wählen Sie auf der Registerkarte **Grundlegende Optionen** unter **Zu scannende Dateien angeben** eine der folgenden Optionen:

- **Alle Dateien scannen** — Legt fest, dass alle Dateien unabhängig vom Dateityp gescannt werden.
- **Standarddateitypen** — Legt fest, dass nur die Standarddateitypen gescannt werden.
- **Definierte Dateitypen** — Legt fest, welche Dateitypen gescannt werden sollen.

6 Wählen Sie unter **Scanneroptionen** die erforderlichen Scanneroptionen aus. Sie haben folgende Möglichkeiten:

- **Archivdateien (ZIP, ARJ, RAR ...) scannen** — Zum Scannen von Archivdateien, z. B. ZIP-Dateien.
- **Unbekannte Dateiviren suchen** — Zur Verwendung heuristischer Analysemethoden zur Suche nach unbekannten Viren.

- **Unbekannte Makroviren suchen** — Zur Suche nach unbekannten Viren in Makros.
- **Alle Dateien nach Makros durchsuchen** — Zum Scannen aller Dateien nach Makros.
- **Alle Makros suchen und als infiziert behandeln** — Zum Suchen nach Makros in Dateien, die dann wie infizierte Elemente behandelt werden.
- **Alle Makros aus Dokumentdateien entfernen** — Zum Entfernen aller Makros aus Dokumentdateien.

7 Geben Sie auf der Registerkarte **Erweitert** unter **Benutzerdefinierte Malwarekategorien** an, welche Elemente als schädliche Software (Malware) behandelt werden. Es stehen zwei Methoden zur Auswahl von Malwaretypen zur Verfügung:

- Wählen Sie die Malwaretypen mithilfe der Kontrollkästchen unter **Benutzerdefinierte Malwarekategorien** aus.
- Wählen Sie **Spezielle Erkennungsnamen**, und klicken Sie auf **Hinzufügen**.

Beim Eingeben eines Namens können Sie Platzhalter für den Mustervergleich verwenden.

8 Aktivieren oder deaktivieren Sie die Option **Keine benutzerdefinierte Malwareprüfung ausführen, wenn das Objekt bereits gesäubert wurde**, um festzulegen, ob Elemente, die bereits erfolgreich gesäubert wurden, bei der Malwareprüfung ebenfalls berücksichtigt werden sollen.

9 Geben Sie unter **Säuberungsoptionen** an, was mit Dateien geschehen soll, die nach dem Säubern ein Größe von 0 Byte aufweisen. Folgende Optionen stehen zur Auswahl:

- **Datei mit null Byte beibehalten** — Gesäuberte Dateien mit einer Größe von 0 Byte werden beibehalten.
- **Datei mit null Byte entfernen** — Dateien mit einer Größe von 0 Byte nach dem Säubern werden entfernt.
- **Als Fehlschlag der Säuberung behandeln** — Dateien mit einer Größe von 0 Byte werden so behandelt, als ob eine Säuberung nicht möglich wäre. Auf diese wird die entsprechende Aktion für fehlgeschlagene Säuberungen angewendet.

10 Unter **Komprimierungsprogramme** stehen folgende Optionen zur Verfügung:

- **Erkennung aktivieren** — Zum Aktivieren oder Deaktivieren der Erkennung von Komprimierungsprogrammen.
- **Angegebene Namen ausschließen** — Zum Angeben der zu ignorierenden Komprimierungsprogramme.

- **Nur angegebene Namen einschließen** — Zum Angeben der Komprimierungsprogramme, die von der Software erkannt werden sollen.
- **Hinzufügen** — Zum Hinzufügen von Namen von Komprimierungsprogrammen zu einer Liste.
- **Löschen** — Zum Löschen von Namen von Komprimierungsprogrammen aus einer Liste.

11 Unter **Potenziell unerwünschte Programme** stehen folgende Optionen zur Verfügung:

Erkennung aktivieren — Zum Aktivieren oder Deaktivieren der Erkennung von potenziell unerwünschten Programmen. Klicken Sie auf den Link zur Verzichtserklärung, und lesen Sie die Verzichtserklärung, bevor Sie die Erkennung potenziell unerwünschter Programme konfigurieren.

Die zu erkennenden Programmtypen auswählen — Zum Angeben, ob die einzelnen Typen von potenziell unerwünschten Programmen erkannt oder ignoriert werden sollen.

- **Spyware**
- **Adware**
- **Remoteverwaltungstools**
- **Dialer**
- **Kennwortcracker**
- **Scherzprogramme**
- **Cookies**
- **Sonstige potenziell unerwünschte Programme**, die nicht in die oben stehenden Kategorien fallen.

Angegebene Namen ausschließen — Zum Auflisten aller potenziell unerwünschten Programme, die von der Software ignoriert werden sollen. Wenn Sie beispielsweise die Erkennung von Spyware aktiviert haben, können Sie eine Liste von Spyware-Programmen erstellen, die von der Software ignoriert werden sollen.

Nur angegebene Namen einschließen — Zum Auflisten aller potenziell unerwünschten Programme, die von der Software erkannt werden sollen. Wenn Sie die Erkennung von Spyware aktivieren und angeben, dass nur benannte Spyware-Programme erkannt werden sollen, werden alle anderen Spyware-Programme ignoriert.

Hinzufügen — Zum Hinzufügen der Namen von potenziell unerwünschten Programmen zu einer Liste. Sie können Platzhalter für Namen verwenden.

Löschen — Zum Löschen hinzugefügter Namen von potenziell unerwünschten Programmen.

Auf der McAfee-Website http://vil.nai.com/vil/default.aspx finden Sie eine Liste mit Namen von potenziell unerwünschten Programmen. Verwenden Sie die Option zum Suchen in Kategorien, um **Potenziell unerwünschte Programme** auszuwählen.

12 Klicken Sie auf **Speichern** und dann auf **Übernehmen**.

Bearbeiten von Antivirenscanner-Aktionen

1 Wählen Sie unter **Richtlinien-Manager** ein Untermenüelement aus, das über einen Antivirenscanner verfügt. Die Richtlinienseite für das Untermenüelement wird angezeigt.

2 Wählen Sie die gewünschte Richtlinie aus.

3 Klicken Sie auf **Antivirenscanner**. Die Registerkarte **Einstellungen anzeigen** für den Antivirenscanner wird angezeigt.

4 Klicken Sie unter dem Abschnitt **Durchzuführende Aktionen** auf den Link **Bearbeiten**. Die Seite **Antivirenscanner-Aktionen** wird angezeigt.

5 Wählen Sie auf der Registerkarte **Säuberung** unter **Säuberung von Viren und Trojanern** die Option **Versuchen, alle erkannten Viren oder Trojaner zu säubern**, um die Säuberung von Viren oder Trojanern zu aktivieren.

6 Wählen Sie unter **Wenn Säuberung erfolgreich, die folgende Aktion durchführen** die gewünschten Optionen aus, falls das Säubern fortgesetzt wird:

- **Protokollieren** — Die Erkennung wird in einer Berichtsdatei protokolliert.
- **Isolieren** — Eine Kopie des Elements wird in einer Quarantäne-Datenbank gespeichert.
- **Administrator benachrichtigen** — Es wird eine Warnmeldung an den E-Mail-Administrator gesendet.
- **Absender benachrichtigen** — Es wird eine Warnmeldung an den Absender gesendet, wenn die Original-E-Mail nicht aus der Domäne stammt, in der Microsoft® Exchange Server 2003/2007 ausgeführt wird.
- **Empfänger benachrichtigen** — Es wird eine Warnmeldung an den Empfänger gesendet, wenn der Empfänger nicht zu der Domäne gehört, in der Microsoft® Exchange Server 2003/2007 ausgeführt wird.

7 Wählen Sie auf den verbleibenden Registerkarten (**Standardaktionen**, **Benutzerdefinierte Malware**, **Komprimierungsprogramme** und **Potenziell unerwünschte Programme**) eine primäre Aktion aus der Dropdown-Liste, und wählen Sie mindestens eine sekundäre Aktion.

Auf der Registerkarte **Benutzerdefinierte Malware** können Sie ebenfalls die benutzerdefinierten Malwarekategorien anzeigen, die Sie während der Erstellung eines neuen Optionssatzes im Antivirenscanner ausgewählt haben (Registerkarte **Erweitert**).

Primäre und sekundäre Antivirenscanner-Aktionen

Primäre Aktionen für den Scan **Bei Zugriff** beinhalten:

- **Element durch Warnung ersetzen** — Ersetzt das Element durch eine Warnmeldung.
- **Eingebettetes Element löschen** — Löscht das erkannte Element. Beispielsweise kann eine Anlage gelöscht werden, die eine Erkennungsregel auslöst.
- **Nachricht löschen** — Löscht die E-Mail.
- **Durchlassen** — Ermöglicht dem Element den Wechsel in die nächste Scanphase oder zum endgültigen Bestimmungsort.

Zu den primären Aktionen für die Scans **Auf Anforderung (Standard)**, **Auf Anforderung (Viren suchen)**, **Auf Anforderung (Viren entfernen)** und **Auf Anforderung (Vollständiger Scan)** zählen Folgende:

- **Element durch Warnung ersetzen** — Ersetzt das Element durch eine Warnmeldung.
- **Nachricht löschen** — Löscht die E-Mail.
- **Durchlassen** — Ermöglicht dem Element den Wechsel in die nächste Scanphase oder zum endgültigen Bestimmungsort.

Sekundäre Aktionen für die Scans **Bei Zugriff** und **Auf Anforderung (Standard)**) beinhalten:

- **Protokollieren** — Die Erkennung wird in einer Berichtsdatei protokolliert.
- **Isolieren** — Eine Kopie des Elements wird in einer Quarantäne-Datenbank gespeichert.
- **Administrator benachrichtigen** — Es wird eine Warnmeldung an den E-Mail-Administrator gesendet.
- **Absender benachrichtigen** — Es wird eine Warnmeldung an den Absender gesendet, wenn die Original-E-Mail nicht aus der Domäne stammt, in der Microsoft® Exchange Server 2003/2007 ausgeführt wird.

- **Empfänger benachrichtigen** — Es wird eine Warnmeldung an den Empfänger gesendet, wenn der Empfänger nicht zu der Domäne gehört, in der Microsoft® Exchange Server 2003/2007 ausgeführt wird.

Sekundäre Aktionen für die Scans **Auf Anforderung (Viren suchen)**, **Auf Anforderung (Viren entfernen)** und **Auf Anforderung (Vollständiger Scan)** beinhalten:

- **Protokollieren** — Die Erkennung wird in einer Berichtsdatei protokolliert.
- **Isolieren** — Eine Kopie des Elements wird in einer Quarantäne-Datenbank gespeichert.
- **Administrator benachrichtigen** — Es wird eine Warnmeldung an den E-Mail-Administrator gesendet.

Inhaltsscan

GroupShield kann Textdaten in E-Mails bzw. Anhängen für das Scannen identifizieren. Sie können Inhaltsregeln erstellen, um gesperrte Inhalte zu definieren und diese den Richtlinien zuweisen.

1. Wählen Sie unter **Richtlinien-Manager** ein Untermenüelement aus, das über den Inhaltsscanner verfügt. Die Richtlinienseite für das Untermenüelement wird angezeigt.
2. Wählen Sie die gewünschte Richtlinie aus der Dropdown-Liste aus.
3. Klicken Sie auf **Inhaltsscan**. Die Registerkarte **Einstellungen anzeigen** für den Inhaltsscanner wird angezeigt.
4. Aktivieren oder deaktivieren Sie unter **Aktivierung** das Kontrollkästchen **Aktivieren**, um die Einstellungen für den Inhaltsscanner für diese Richtlinie ein- oder auszuschalten.
5. Wählen Sie unter **Optionen** Folgendes aus:
   - **Dokument- und Datenbankformate in Inhaltsscans einbeziehen**
   - **Text aller Anlagen scannen**
6. Wählen Sie unter **Beim Ersetzen von Text aufgrund der Auslösung einer Regel die folgende Warnung verwenden** eine vorhandene Warnung aus dem Dropdown-Menü, oder klicken Sie auf **Erstellen**, um eine neue Warnung zu erstellen.

Schrittweise Anleitungen zum Erstellen neuer Warnungen finden Sie unter *Erstellen einer neuen Warnung auf Seite 133*.

Wenn der Text der Warnmeldung nicht angezeigt wird, Sie ihn jedoch in einer Vorschau anzeigen möchten, klicken Sie auf **Anzeigen/Ausblenden**, um den Text anzuzeigen. Wenn der Text der Warnmeldung angezeigt wird, klicken Sie auf **Anzeigen/Ausblenden**, um ihn auszublenden.

Standardwarnungen können nicht bearbeitet werden, da sie schreibgeschützt sind.

7 Unter **Regeln und zugeordnete Aktionen für Inhaltsscanner** stehen folgende Möglichkeiten zur Verfügung:

- **Regel hinzufügen** — Zum Erstellen einer neuen Inhaltsregel für diese Richtlinie.

Schrittweise Anleitungen zum Erstellen neuer Inhaltsregeln finden Sie unter *Hinzufügen einer neuen Inhaltsregel auf Seite 135*.

- **Bearbeiten** — Zum Ändern der mit einer Inhaltsregel verknüpften Aktion.
- **Löschen** — Zum Löschen der Inhaltsregel.

Erstellen einer neuen Warnung

1 Wählen Sie unter **Richtlinien-Manager** ein Untermenüelement aus. Die Richtlinienseite für das Untermenüelement wird angezeigt.

2 Wählen Sie die gewünschte Richtlinie aus.

3 Klicken Sie auf **Inhaltsscan**. Die Registerkarte **Einstellungen anzeigen** für den Inhaltsscanner wird angezeigt.

4 Klicken Sie unter **Optionen** auf **Erstellen**. Die Seite **Warnungseditor** wird angezeigt.

5 Geben Sie unter **Warnungsname** einen sinnvollen Namen ein.

6 Wählen Sie unter **Warnung für Inhaltsscans** die gewünschten Einstellungen für **Stil**, **Schriftart**, **Größe** und **Token** in den jeweiligen Dropdown-Listen aus.

Diese Optionen stehen nur zur Verfügung, wenn Sie **HTML-Inhalt (WYSIWYG)** aus dem Dropdown-Menü **Anzeigen** auswählen.

7 Wählen Sie unter **Warnung für Inhaltsscans** die gewünschten Tools aus.

- **Fett** — Formatiert den ausgewählten Text fett.
- **Kursiv** — Formatiert den ausgewählten Text kursiv.

- **Unterstrichen** — Unterstreicht den ausgewählten Text.
- **Linksbündig** — Richtet den markierten Absatz linksbündig aus.
- **Zentriert** — Richtet den markierten Absatz in der Mitte aus.
- **Rechtsbündig** — Richtet den markierten Absatz rechtsbündig aus.
- **Blocksatz** — Formatiert den markierten Absatz im Blocksatz (rechts- und linksbündig).
- **Geordnete Liste** — Wandelt den markierten Text in eine nummerierte Liste um.
- **Ungeordnete Liste** — Wandelt den markierten Text in eine Liste mit Aufzählungszeichen um.
- **Auszug** — Verschiebt den markierten Text um einen vorgegebenen Abstand nach rechts.
- **Einzug** — Verschiebt den markierten Text um einen vorgegebenen Abstand nach links.
- **Textfarbe** — Ändert die Farbe des markierten Textes.
- **Hintergrundfarbe** — Ändert die Hintergrundfarbe des markierten Textes.
- **Horizontales Lineal** — Fügt eine horizontale Linie ein.
- **Link einfügen** — Fügt einen Hyperlink an der aktuellen Cursorposition ein. Geben Sie in das Feld **URL** den URL ein. Geben Sie in das Feld **Text** den Namen für den Hyperlink ein, wie er in der Warnung angezeigt werden soll. Wenn durch Klicken auf den Link ein neues Fenster geöffnet werden soll, wählen Sie **Link in neuem Fenster öffnen** aus, und klicken Sie dann auf **Link einfügen**.
- **Bild einfügen** — Fügt ein Bild an der aktuellen Cursorposition ein. Geben Sie in das Feld **Bild-URL** den Pfad für das Bild ein. Geben Sie in das Feld **Alternativer Text** den Text ein, der angezeigt werden soll, wenn Bilder unterdrückt werden oder die Warnung mit einem Nur-Text-Browser angezeigt wird. Wenn Sie das Bild mit einem Titel versehen möchten, geben Sie den Namen des Titels in das Feld **Diesen Text als Bildtitel verwenden** ein. Klicken Sie auf **Bild einfügen**.
- **Tabelle einfügen** — Fügt eine Tabelle an der aktuellen Cursorposition ein. Geben Sie die Werte in die Felder **Zeilen**, **Spalten**, **Tabellenbreite**, **Rahmenbreite**, **Textabstand** und **Zellenabstand** ein, um die Tabelle zu konfigurieren, und klicken Sie dann auf **Tabelle einfügen**.

8 Legen Sie im Dropdown-Menü **Anzeigen** fest, wie die Warnmeldung auf der Benutzeroberfläche angezeigt werden soll. Sie haben folgende Möglichkeiten:

- **HTML-Inhalt (WYSIWYG)** — Blendet den zugrunde liegenden HTML-Code aus, sodass nur der Inhalt der Warnung angezeigt wird.
- **HTML-Inhalt (Quelle)** — Zeigt den HTML-Code vor der Kompilierung an.
- **Einfacher Textinhalt** — Zeigt den Text als unformatierten Text an.

9 Klicken Sie auf **Speichern** und dann auf **Übernehmen**.

Klicken Sie auf **Zurücksetzen**, um alle Änderungen seit dem letzten Speichern der Warnmeldung rückgängig zu machen.

Hinzufügen einer neuen Inhaltsregel

1 Wählen Sie unter **Richtlinien-Manager** ein Untermenüelement aus. Die Richtlinienseite für das Untermenüelement wird angezeigt.

2 Wählen Sie die gewünschte Richtlinie aus.

3 Klicken Sie auf **Inhaltsscan**. Die Registerkarte **Einstellungen anzeigen** für den Inhaltsscanner wird angezeigt.

4 Klicken Sie unter **Regeln und zugeordnete Aktionen für Inhaltsscanner** auf **Regel hinzufügen**. Die Seite **Inhaltsregeln** wird angezeigt.

5 Führen Sie unter **Aktionen für eine Auswahl von Inhaltsregeln angeben** folgende Aktionen durch:

- Wählen Sie eine Regelgruppe im Dropdown-Menü **Regelgruppe auswählen** aus, die eine Aktion auslöst, wenn mindestens eine ihrer Regeln verletzt wurde.
- Legen Sie unter **Regeln aus dieser Gruppe auswählen** fest, ob alle Regeln oder nur Regeln mit einem bestimmten Schweregrad eingebunden werden sollen. Die verfügbaren Optionen lauten **Schweregrad - Niedrig**, **Schweregrad - Mittel**, und **Schweregrad - Hoch**.

Die Auswahl der Option **Alle auswählen** überschreibt alle drei Regeln.

6 Wählen Sie unter **Bei Erkennung die folgende Aktion durchführen** die gewünschten primären und sekundären Inhaltsscanner-Aktionen aus.

Weitere Informationen hierzu finden Sie unter *Primäre und sekundäre Inhaltsscanner-Aktionen auf Seite 136*.

7 Klicken Sie auf **Speichern** und dann auf **Übernehmen**.

Primäre und sekundäre Inhaltsscanner-Aktionen

Primäre Aktionen für den Scan **Bei Zugriff** beinhalten:

- **Element durch Warnung ersetzen** — Ersetzt das erkannte Element durch eine Warnmeldung.
- **Eingebettetes Element löschen** — Löscht das erkannte Element. Beispielsweise kann eine Anlage gelöscht werden, die eine Erkennungsregel auslöst.
- **Nachricht löschen** — Löscht die E-Mail.
- **Durchlassen** — Ermöglicht dem Element den Wechsel in die nächste Scanphase oder zum endgültigen Bestimmungsort.

Zu den primären Aktionen für die Scans **Auf Anforderung (Standard)**, **Auf Anforderung (Gesperrte Inhalte suchen)**, **Auf Anforderung (Gesperrte Inhalte entfernen)** und **Auf Anforderung (Vollständiger Scan)** zählen Folgende:

- **Element durch Warnung ersetzen** — Ersetzt das Element durch eine Warnmeldung.
- **Nachricht löschen** — Löscht die E-Mail.
- **Durchlassen** — Ermöglicht dem Element den Wechsel in die nächste Scanphase oder zum endgültigen Bestimmungsort.

Sekundäre Aktionen für die Scans **Bei Zugriff** und **Auf Anforderung (Standard)**) beinhalten:

- **Protokollieren** — Die Erkennung wird in einer Berichtsdatei protokolliert.
- **Isolieren** — Eine Kopie des Elements wird in einer Quarantäne-Datenbank gespeichert.
- **Administrator benachrichtigen** — Es wird eine Warnmeldung an den E-Mail-Administrator gesendet.
- **Absender benachrichtigen** — Es wird eine Warnmeldung an den Absender gesendet, wenn die Original-E-Mail nicht aus der Domäne stammt, in der Microsoft® Exchange Server 2003/2007 ausgeführt wird.
- **Empfänger benachrichtigen** — Es wird eine Warnmeldung an den Empfänger gesendet, wenn der Empfänger nicht zu der Domäne gehört, in der Microsoft® Exchange Server 2003/2007 ausgeführt wird.

Sekundäre Aktionen für die Scans **Auf Anforderung (Gesperrte Inhalte suchen)**, **Auf Anforderung (Gesperrte Inhalte entfernen)** und **Auf Anforderung (Vollständiger Scan)** beinhalten:

- **Protokollieren** — Die Erkennung wird in einer Berichtsdatei protokolliert.
- **Isolieren** — Eine Kopie des Elements wird in einer Quarantäne-Datenbank gespeichert.
- **Administrator benachrichtigen** — Es wird eine Warnmeldung an den E-Mail-Administrator gesendet.

Dateifilterung

Sie können die Dateifiltereinstellungen für eine bestimmte Richtlinie konfigurieren.

1. Wählen Sie unter **Richtlinien-Manager** ein Untermenüelement aus, das über einen Dateifilter verfügt. Die Richtlinienseite für das Untermenüelement wird angezeigt.
2. Wählen Sie die gewünschte Richtlinie aus.
3. Klicken Sie auf **Dateifilterung**. Die Registerkarte **Einstellungen anzeigen** für den Dateifilterungsscanner wird angezeigt.
4. Aktivieren oder deaktivieren Sie unter **Aktivierung** das Kontrollkästchen **Aktivieren**, um die Einstellungen für den Dateifilterungsscanner für die Richtlinie ein- oder auszuschalten.
5. Geben Sie unter **Warnungsauswahl** an, welche Warnmeldung verwendet wird, wenn eine infizierte E-Mail eine Dateifilterregel auslöst. Sie haben auch die Möglichkeit, eine vorhandene Warnung auszuwählen, oder über **Erstellen** eine neue Warnung zu erstellen.

Schrittweise Anleitungen zum Erstellen neuer Warnungen finden Sie unter *Erstellen einer neuen Warnung auf Seite 133*.

Wenn der Text der Warnmeldung nicht angezeigt wird, Sie ihn jedoch in einer Vorschau anzeigen möchten, klicken Sie auf **Anzeigen/Ausblenden**, um den Text anzuzeigen. Wenn der Text der Warnmeldung angezeigt wird, klicken Sie auf **Anzeigen/Ausblenden**, um ihn auszublenden.

6 Unter **Regeln und zugeordnete Aktionen für Dateifilterung** stehen folgende Optionen zur Verfügung:

- **Verfügbare Regeln** — Ermöglicht die Auswahl einer bestehenden Dateifilterregel oder das Erstellen einer neuen Dateifilterregel für die Richtlinie. Wählen Sie zum Erstellen einer neuen Dateifilterregel **Neue Regel erstellen** aus. Die Seite **Dateifilterregel** wird angezeigt. Mit den Dateifilterregeln können Sie die Dateibewegungen überwachen und einschränken. Sie können die Dateien sogar nach Name, Kategorietyp und Größe filtern.

Weitere Informationen zu **Neue Regel erstellen** finden Sie unter *Erstellen einer neuen Dateifilterregel auf Seite 138*.

- **Ändern** – Ändert die einer Dateifilterregel zugewiesenen primären und sekundären Aktionen.

Weitere Informationen zum Ändern der einer Dateifilterregel zugewiesenen primären und sekundären Aktionen finden Sie unter *Primäre und sekundäre Dateifilteraktionen auf Seite 140*.

- **Löschen** — Löscht die Dateifilterregel.

Erstellen einer neuen Dateifilterregel

1 Wählen Sie unter **Richtlinien-Manager** ein Untermenüelement aus, das über einen Dateifilter verfügt. Die Richtlinienseite für das Untermenüelement wird angezeigt.

2 Wählen Sie die gewünschte Richtlinie aus.

3 Klicken Sie auf **Dateifilterung**. Die Registerkarte **Einstellungen anzeigen** für den Dateifilterungsscanner wird angezeigt.

4 Wählen Sie im Dropdown-Menü **Verfügbar Regeln** unter **Regeln und zugeordnete Aktionen für Dateifilterung** die Option **Neue Regel erstellen** aus. Die Seite **Dateifilterregel** wird angezeigt.

5 Geben Sie unter **Regelnamen** einen eindeutigen Namen für diese Regel ein. Der Name sollte aussagekräftig sein, damit Regel und Funktionsweise leicht zu erkennen sind.
Beispiel: DateienÜber5MB.

6 Wählen Sie unter **Filterung von Dateinamen** die Option **Filterung von Dateinamen aktivieren** aus, um Dateien nach Namen zu filtern.
Wenn Sie beispielsweise ***.exe** eingeben, wird diese Dateifilterregel auf alle Dateien mit der Erweiterung EXE angewendet.

7 Geben Sie unter **Aktion durchführen, wenn Dateiname übereinstimmt mit** die Namen der Dateien an, die von dieser Regel berücksichtigt werden.
Verwenden Sie die Platzhalterzeichen * und ?, um Übereinstimmungen für mehrere Dateinamen zu finden. Wenn Sie beispielsweise nach ausführbaren Dateien filtern möchten, geben Sie „*.exe“ ein.

8 Klicken Sie auf **Hinzufügen**, um die Dateinamen der Filterliste hinzuzufügen, oder auf **Löschen**, um sie aus der Liste zu entfernen.

9 Wählen Sie unter **Filterung von Dateikategorien** die Option **Filterung von Dateikategorien aktivieren** aus, um Dateien nach Dateityp zu filtern.

10 Geben Sie unter **Aktion bei folgender Dateikategorie durchführen** den Typ der Dateien an, die von dieser Regel berücksichtigt werden.

Dateitypen werden in Kategorien und Unterkategorien aufgeteilt.

11 Klicken Sie unter **Dateikategorien** auf einen Dateityp. Neben dem Dateityp wird ein Sternchen (*) als Hinweis darauf angezeigt, dass nach diesem Dateityp gefiltert wird.

12 Klicken Sie unter **Unterkategorien** auf die zu filternde Unterkategorie.

Verwenden Sie die UMSCHALT- oder die STRG-TASTE, um mehrere Unterkategorien auszuwählen. Zur Auswahl sämtlicher Unterkategorien, klicken Sie auf **Alle**.

Klicken Sie auf **Auswahl löschen**, um die letzte Auswahl rückgängig zu machen. Klicken Sie auf die gewünschte, ausgewählte **Dateikategorie** (mit Sternchen), und klicken Sie zum Aufheben der Auswahl auf **Auswahl löschen**.

13 Wählen Sie **Diese Regel auf unbekannte Dateikategorien erweitern** aus, um diese Regel auf alle anderen Dateikategorien und Unterkategorien anzuwenden, die nicht speziell in der Liste der Kategorien und Unterkategorien aufgelistet sind.

14 Wählen Sie unter **Dateigrößenfilterung** die Option **Dateigrößenfilterung aktivieren** aus, um Dateien nach Größe zu filtern.

15 Wählen Sie unter **Aktion bei folgender Dateigröße durchführen** die Option **Größer als** aus, um festzulegen, dass die Aktion nur angewendet wird, wenn die Datei eine bestimmte Größe übersteigt.

16 Wählen Sie **Kleiner als**, wenn die Aktion nur bei Dateien angewendet werden soll, die eine bestimmte Größe unterschreiten.

17 Klicken Sie auf **Speichern** und dann auf **Übernehmen**.

Primäre und sekundäre Dateifilteraktionen

Primäre Aktionen für den Scan **Bei Zugriff** beinhalten:

- **Element durch Warnung ersetzen** — Ersetzt das Element durch eine Warnmeldung.
- **Eingebettetes Element löschen** — Löscht das erkannte Element. Beispielsweise kann eine Anlage gelöscht werden, die eine Erkennungsregel auslöst.
- **Nachricht löschen** — Löscht die E-Mail.
- **Durchlassen** — Ermöglicht dem Element den Wechsel in die nächste Scanphase oder zum endgültigen Bestimmungsort.

Primäre Aktionen für die Scans **Auf Anforderung (Standard)** und **Auf Anforderung (Vollständiger Scan)** beinhalten:

- **Element durch Warnung ersetzen** — Ersetzt das Element durch eine Warnmeldung.
- **Nachricht löschen** — Löscht die E-Mail.
- **Durchlassen** — Ermöglicht dem Element den Wechsel in die nächste Scanphase oder zum endgültigen Bestimmungsort.

Sekundäre Aktionen für die Scans **Bei Zugriff** und **Auf Anforderung (Standard)**) beinhalten:

- **Protokollieren** — Die Erkennung wird in einer Berichtsdatei protokolliert.
- **Isolieren** — Eine Kopie des Elements wird in einer Quarantäne-Datenbank gespeichert.
- **Administrator benachrichtigen** — Es wird eine Warnmeldung an den E-Mail-Administrator gesendet.
- **Absender benachrichtigen** — Es wird eine Warnmeldung an den Absender gesendet, wenn die Original-E-Mail nicht aus der Domäne stammt, in der Microsoft® Exchange Server 2003/2007 ausgeführt wird.
- **Empfänger benachrichtigen** — Es wird eine Warnmeldung an den Empfänger gesendet, wenn der Empfänger nicht zu der Domäne gehört, in der Microsoft® Exchange Server 2003/2007 ausgeführt wird.

Sekundäre Aktionen für den Scan **Auf Anforderung (Vollständiger Scan)** beinhalten:

- **Protokollieren** — Die Erkennung wird in einer Berichtsdatei protokolliert.
- **Isolieren** — Eine Kopie des Elements wird in einer Quarantäne-Datenbank gespeichert.
- **Administrator benachrichtigen** — Es wird eine Warnmeldung an den E-Mail-Administrator gesendet.

Anti-Spam

Sie können die Dateifiltereinstellungen für eine bestimmte Richtlinie konfigurieren.

1 Wählen Sie unter **Richtlinien-Manager** die Option **Gateway**. Die Richtlinienseite für **Gateway** wird angezeigt.

2 Wählen Sie die gewünschte Richtlinie aus.

3 Klicken Sie auf **Anti-Spam**. Die Registerkarte **Einstellungen anzeigen** für den Anti-Spam-Scanner wird angezeigt.

4 Aktivieren oder deaktivieren Sie unter **Aktivierung** das Kontrollkästchen **Aktivieren**, um die Anti-Spam-Einstellungen für die Richtlinie ein- oder auszuschalten.

5 Wählen Sie unter **Optionen** eine der folgenden Optionen aus:

- **Kerneinstellungen für Anti-Spam** — Wird zum Anzeigen und Konfigurieren der standardmäßigen Anti-Spam-Einstellungen verwendet.
- **neuen Optionssatz erstellen** — Ermöglicht das Erstellen eines neuen Optionssatzes für Anti-Spam-Einstellungen.

Weitere Informationen hierzu finden Sie unter *Erstellen eines neuen Optionssatzes für Anti-Spam-Einstellungen auf Seite 142*.

- **Bearbeiten** — Ermöglicht die Änderung der Optionen von Anti-Spam-Einstellungen, die mit einer Richtlinie verknüpft sind.

6 Klicken Sie unter **Durchzuführende Aktionen bei Erkennung von Spam** auf **Bearbeiten**. Die Seite **Anti-Spam-Aktion** wird mit drei Registerkarten angezeigt:

- **Hoher Faktor**
- **Mittlerer Faktor**
- **Geringer Faktor**

7 Wählen Sie basierend auf dem Spamfaktor (**Hoch**, **Medium** or **Gering**) die gewünschten primären und sekundären Aktionen auf allen Registerkarten aus.

Der Anti-Spam-Scanner wird nur auf eingehende E-Mails angewendet.

Primäre und sekundäre Filteraktionen für Anti-Spam

Primäre Aktionen für den Scan **Gateway** (für den hohen, mittleren und geringen Spamfaktor) beinhalten:

- **In Systemmüllordner weiterleiten** — E-Mails werden in den Systemmüllordner weitergeleitet.
- **In Benutzermüllordner weiterleiten** — E-Mails werden in den Benutzermüllordner weitergeleitet.
- **Nachricht ablehnen** — Die E-Mail wird abgelehnt.
- **Nachricht löschen** — Die E-Mail wird gelöscht.
- **Durchlassen** — Ermöglicht dem Element den Wechsel in die nächste Scanphase oder zum endgültigen Bestimmungsort.

Sekundäre Aktionen für den Scan **Gateway** (für den hohen, mittleren und geringen Spamfaktor) beinhalten:

- **Protokollieren** — Die Erkennung wird in einer Berichtsdatei protokolliert.
- **Nachricht isolieren** — Eine Kopie des Elements wird in einer Quarantäne-Datenbank gespeichert.
- **Administrator benachrichtigen** — Es wird eine Warnmeldung an den E-Mail-Administrator gesendet.

Erstellen eines neuen Optionssatzes für Anti-Spam-Einstellungen

1. Wählen Sie unter **Richtlinien-Manager** die Option **Gateway**. Die Richtlinienseite für das Untermenüelement **Gateway** wird angezeigt.
2. Wählen Sie die gewünschte Richtlinie aus der Dropdown-Liste aus.
3. Klicken Sie auf **Anti-Spam**. Die Registerkarte **Einstellungen anzeigen** für den Anti-Spam-Scanner wird angezeigt.
4. Geben Sie unter **Instanzname** einen Namen für die Anti-Spam-Einstellungen ein. Dieses Feld muss ausgefüllt werden.
5. Klicken Sie im Dropdown-Menü **Optionen** auf **neuen Optionssatz erstellen**. Die Seite **Anti-Spam-Einstellungen** wird mit vier Registerkarten angezeigt:
   - **Optionen**
   - **Erweitert**
   - **Nachrichtenlisten**
   - **Regeln**

6 Geben Sie auf der Registerkarte **Optionen** unter **Faktoren** folgende Werte ein:

- **Schwellenwert für Faktor 'Hoch'** — Wenn der Gesamt-Spamfaktor gleich oder größer als 15 ist.
- **Schwellenwert für Faktor 'Mittel'** — Wenn der Gesamt-Spamfaktor gleich oder größer als 10, aber kleiner als 15 ist.
- **Schwellenwert für Faktor 'Gering'** — Wenn der Gesamt-Spamfaktor gleich oder größer als 5, aber kleiner als 10 ist.

Um die Standardwerte von Spamfaktoren zu verwenden, wählen Sie die Option **Standard verwenden**.

Die Standardeinstellungen wurden nach sorgfältiger Analyse definiert, um ein ausgewogenes Verhältnis zwischen einer hohen Spamerkennungsrate und einer niedrigen Rate an falschen Alarmen zu erzielen. Für den unwahrscheinlichen Fall, dass Sie die Einstellungen ändern müssen, bietet der Technische Support entsprechende technische Unterlagen.

7 Wählen Sie unter **Berichtserstellung** im Dropdown-Menü **Der Schwellenwert für die Erstellung von Spamberichten beträgt** die Option **Hoch**, **Mittel**, **Gering** oder **Benutzerdefiniert** aus, um anzugeben, ab wann eine E-Mail als Spam gekennzeichnet werden sollte.

8 Geben Sie unter **Benutzerdefinierter Faktor** einen speziellen Spamfaktor ein, bei dem eine E-Mail als Spam gekennzeichnet wird. Dieses Feld ist nur aktiviert, wenn Sie in Schritt 6 die Option **Benutzerdefiniert** auswählen.

9 Wählen Sie die Option **Präfix zum Betreff von Spamnachrichten hinzufügen** aus, oder heben Sie die Auswahl auf.

10 Wählen Sie im Dropdown-Menü zum Hinzufügen der Anzeige für den Spamfaktor eine der folgenden Optionen aus:

- **Nie** — In den Internet-Kopfzeilen von E-Mails wird unter keinen Umständen die Anzeige für den Spamfaktor hinzugefügt.
- **Nur zu Spamnachrichten** — Nur in den Internet-Kopfzeilen von Spam-E-Mails wird die Anzeige für den Spamfaktor hinzugefügt.
- **Nur zu Nicht-Spamnachrichten** — Nur in den Kopfzeilen von Nicht-Spam-E-Mails wird die Anzeige für den Spamfaktor hinzugefügt.

- **Zu allen Nachrichten** — In den Kopfzeilen aller E-Mails wird die Anzeige für den Spamfaktor hinzugefügt.

Bei der Anzeige des Spamfaktors handelt es sich um ein Symbol im Spambericht, das in die Internet-Kopfzeile der E-Mail eingefügt wird und den Spamanteil in einer E-Mail anzeigt.

11 Wählen Sie im Dropdown-Menü **Spambericht anhängen** eine der folgenden Optionen aus:

- **Nie** — E-Mails wird unter keine Umständen ein Spambericht hinzugefügt.
- **Nur zu Spamnachrichten** — Nur Spam-E-Mails wird ein Spambericht hinzugefügt.
- **Nur zu Nicht-Spamnachrichten** — Nur Nicht-Spam-E-Mails wird ein Spambericht hinzugefügt.
- **Zu allen Nachrichten** — Allen E-Mails wird ein Spambericht hinzugefügt.

12 Wählen Sie die Option **Ausführliche Berichte** aus, oder heben Sie ihre Auswahl auf, um anzugeben, ob ausführliche Berichte erforderlich sind.
In ausführlichen Berichten sind die Namen und Beschreibungen der Anti-Spam-Regeln enthalten, die ausgelöst wurden.

Ausführliche Berichte steht nur zur Verfügung, wenn Sie in Schritt 10 nicht **Nie** auswählen.

13 Auf der Registerkarte **Erweitert** stehen folgende Optionen zur Verfügung:

- **Maximale Gesamtnachrichtengröße (KB)** — Zum Angeben der maximal zulässigen Größe einer scanbaren E-Mail (in KB). Sie können eine Größe bis 999.999.999 KB eingeben, obwohl Spam-E-Mails üblicherweise recht klein sind. Der Standardwert ist 250.
- **Maximale Breite von Spamkopfzeilen (Byte)** — Zum Angeben der maximal zulässigen Größe der Kopfzeile einer Spam-E-Mail (in Byte). Die minimale Breite von Spamkopfzeilen kann 40 Zeichen und die maximale 999 Zeichen betragen. Der Standardwert ist 76.

Um ihr Ziel zu erreichen, fügen Spammer häufig Zusatzinformationen in Kopfzeilen ein.

- **Maximale Anzahl von gemeldeten Regeln** — Zum Angeben der maximalen Anzahl von Anti-Spam-Regeln, die in einen Spambericht aufgenommen werden können. Die minimale Anzahl von Regeln kann 1 und die maximale 999 sein. Der Standardwert ist 180.

- **Kopfzeilenname** — Zum Angeben eines anderen Namens für die E-Mail-Kopfzeile. Sie können die Kopfzeile und den Kopfzeilenwert (unten) beim Nachverfolgen von E-Mails und Anwenden von Regeln auf diese Nachrichten verwenden. Diese Felder sind optional und akzeptieren bis zu 40 Zeichen.
- **Kopfzeilenwert** — Zum Angeben eines anderen Kopfzeilenwertes für die E-Mail-Kopfzeile.
- **Kopfzeile hinzufügen** — Zum Angeben, dass die Kopfzeile zu keiner E-Mail, zu allen E-Mails, nur zu Spam-E-Mails oder nur zu Nicht-Spam-E-Mails hinzugefügt werden soll.
- Wählen Sie die Option **Alternative Kopfzeilennamen verwenden, wenn Nachricht kein Spam ist** aus, oder heben Sie ihre Auswahl auf.
- Wählen Sie in der Dropdown-Liste **Spamprofil** das erforderliche Spamprofil aus.

Ein Spamprofil enthält eine Reihe von Merkmalen einer bestimmten Spamkategorie. Um Anti-Spam-Programmen eine bessere Erkennung von Spam zu ermöglichen, können Benutzer Spam-Muster einsenden, anhand derer die Software lernt und Spam zukünftig noch effektiver erkennt. Die Anti-Spam-Software erzeugt ein Spamprofil, in dem alle Merkmale aufgeführt sind, die die Benutzer als spamtypisch erachten.

14 Geben Sie auf der Registerkarte **Nachrichtenlisten** unter **Schwarze Listen** und **Weiße Listen** die E-Mail-Adressen der Absender und Empfänger ein, die auf den schwarzen und weißen Listen stehen.
E-Mails, die von Adressen oder an Adressen gesendet werden, die in einer schwarzen Liste enthalten sind, werden unabhängig vom Inhalt als Spam behandelt. E-Mails, die von Adressen oder an Adressen gesendet werden, die in einer weißen Liste enthalten sind, werden unabhängig vom Inhalt niemals als Spam behandelt.

Klicken Sie auf **Hinzufügen**, um einer Liste E-Mail-Adressen hinzuzufügen, und aktivieren oder deaktivieren Sie das Kontrollkästchen neben den einzelnen Adressen, um anzugeben, ob sie momentan aktiviert sind. Klicken Sie auf **Löschen**, um eine E-Mail-Adresse aus der Liste zu entfernen.

Dieselbe E-Mail-Adresse kann nicht mehrmals hinzugefügt werden.

15 Klicken Sie auf der Registerkarte **Regeln** auf den Link **Bearbeiten** einer Regel, um sie zu aktivieren oder zu deaktivieren und ihren Spamfaktor zu ändern. Klicken Sie dann auf den Link **Speichern** der entsprechende Regel.

Klicken Sie auf **Zurücksetzen**, um zu den standardmäßigen Anti-Spam-Einstellungen zurückzukehren.

16 Klicken Sie auf **Speichern** und dann auf **Übernehmen**.

Anti-Phishing

Sie können die Anti-Phishing-Einstellungen für eine bestimmte Richtlinie konfigurieren.

1 Wählen Sie unter **Richtlinien-Manager** die Option **Gateway**. Die Richtlinienseite für **Gateway** wird angezeigt.

2 Wählen Sie die gewünschte Richtlinie aus.

3 Klicken Sie auf **Anti-Phishing**. Die Registerkarte **Einstellungen anzeigen** für das Anti-Phishing wird angezeigt.

4 Aktivieren oder deaktivieren Sie unter **Aktivierung** das Kontrollkästchen **Aktivieren**, um die Anti-Phishing-Einstellungen für die Richtlinie ein- oder auszuschalten.

5 Wählen Sie im Dropdown-Menü **Optionen** eine der folgenden Optionen aus:

- **Kerneinstellungen für Anti-Phishing** — Wird zum Anzeigen und Konfigurieren der standardmäßigen Anti-Phishing-Einstellungen verwendet.
- **neuen Optionssatz erstellen** — Ermöglicht das Erstellen eines neuen Optionssatzes für Anti-Phishing-Einstellungen.

Weitere Informationen hierzu finden Sie unter *Erstellen eines neuen Optionssatzes für Anti-Phishing-Einstellungen auf Seite 147*.

- **Bearbeiten** — Ermöglicht die Änderung der Optionen von Anti-Phishing-Einstellungen, die mit einer Richtlinie verknüpft sind.

6 Klicken Sie unter **Aktionen** auf **Bearbeiten**. Die Seite **Anti-Phishing-Aktionen** wird angezeigt.

7 Wählen Sie die gewünschten primären und sekundären Aktionen aus.

Der Anti-Phishing-Scanner wird nur auf eingehende E-Mails angewendet.

Primäre und sekundäre Filteraktionen für Anti-Phishing

Primäre Aktionen für den Scan **Gateway** (für den hohen, mittleren und geringen Spamfaktor) beinhalten:

- **Nachricht ablehnen** — Die E-Mail wird abgelehnt.
- **Nachricht löschen** — Die E-Mail wird gelöscht.
- **Durchlassen** — Dem Element wird der Wechsel in die nächste Scanphase oder zum endgültigen Bestimmungsort ermöglicht.

Sekundäre Aktionen für den Scan **Gateway** (für den hohen, mittleren und geringen Spamfaktor) beinhalten:

- **Protokollieren** — Die Erkennung wird in einer Berichtsdatei protokolliert.
- **Nachricht isolieren** — Eine Kopie des Elements wird in einer Quarantäne-Datenbank gespeichert.
- **Administrator benachrichtigen** — Es wird eine Warnmeldung an den E-Mail-Administrator gesendet.

Erstellen eines neuen Optionssatzes für Anti-Phishing-Einstellungen

1. Wählen Sie unter **Richtlinien-Manager** die Option **Gateway**. Die Richtlinienseite für das Untermenüelement **Gatway** wird angezeigt.
2. Wählen Sie die gewünschte Richtlinie aus der Dropdown-Liste aus.
3. Klicken Sie auf **Anti-Phishing**. Die Registerkarte **Einstellungen anzeigen** für den Anti-Phishing-Scanner wird angezeigt.
4. Klicken Sie im Dropdown-Menü **Optionen** auf **neuen Optionssatz erstellen**. Die Seite **Anti-Phishing-Einstellungen** wird angezeigt.
5. Geben Sie unter **Instanzname** einen Namen für die Anti-Phishing-Einstellungen ein. Dieses Feld muss ausgefüllt werden.
6. Wählen Sie unter **Berichtserstellung** die folgenden Optionen aus:
   - **Präfix zum Betreff von Phishing-Nachrichten hinzufügen** — Gibt an, dass Sie am Anfang der Betreffzeile einer als Phishing-Nachricht verdächtigten E-Mail Text einfügen möchten.
   - **Kopfzeile mit Phishinghinweis zu Nachrichten hinzufügen** — Gibt an, ob ein Phishinghinweis zur Kopfzeile einer als Phishing-Nachricht verdächtigten E-Mail hinzugefügt werden soll.
   - **Phishingbericht anhängen** — Gibt an, ob ein Phishingbericht erzeugt und an die E-Mail angehängt werden soll.
   - **Ausführliche Berichte** — Gibt an, ob die Namen und Beschreibungen der ausgelösten Anti-Phishing-Regeln in die E-Mail aufgenommen werden sollen. Diese Option steht nur bei ausgewählter Option **Phishingbericht anhängen** zur Verfügung.
7. Klicken Sie auf **Speichern** und dann auf **Übernehmen**.

Filter

GroupShield 7.0 beinhaltet folgende Filter:

- **Beschädigter Inhalt**
- **Geschützter Inhalt**
- **Verschlüsselter Inhalt**
- **Signierter Inhalt**
- **Kennwortgeschützte Dateien**
- **Scannersteuerung**
- **Einstellungen für MIME-Nachrichten.**
- **HTML-Dateien**
- **Nachrichtengrößenfilterung**

Beschädigter Inhalt

Der Inhalt in einigen E-Mails kann beschädigt sein. Er kann dann nicht gescannt werden. Die Richtlinie für beschädigten Inhalt legt fest, wie E-Mails mit beschädigtem Inhalt bei Erkennung behandelt werden.

1 Wählen Sie unter **Richtlinien-Manager** ein Untermenüelement aus. Die Richtlinienseite für das Untermenüelement wird angezeigt.

2 Wählen Sie die gewünschte Richtlinie aus.

3 Klicken Sie auf **Beschädigter Inhalt**. Die Registerkarte **Einstellungen anzeigen** für den Filter für beschädigten Inhalt wird angezeigt.

4 Aktivieren oder deaktivieren Sie unter **Aktivierung** das Kontrollkästchen **Aktivieren**, um die Einstellungen für den Filter für beschädigten Inhalt für die Richtlinie ein- oder auszuschalten.

5 Zeigen Sie unter **Aktionen** die Aktion an, die bei Erkennung von beschädigtem Inhalt durchgeführt werden soll.
Klicken Sie zum Ändern dieser Aktionen auf den Link **Bearbeiten**.

Informationen zum Bearbeiten der Aktionen, die bei Erkennung von beschädigtem Inhalt durchgeführt werden sollen, finden Sie unter *Primäre und sekundäre Filteraktionen für beschädigten Inhalt auf Seite 149*.

Primäre und sekundäre Filteraktionen für beschädigten Inhalt

Primäre Aktionen für den Scan **Bei Zugriff** beinhalten:

- **Element durch Warnung ersetzen** — Ersetzt das Element durch eine Warnmeldung.
- **Eingebettetes Element löschen** — Löscht das erkannte Element. Beispielsweise kann eine Anlage gelöscht werden, die eine Erkennungsregel auslöst.
- **Nachricht löschen** — Löscht die E-Mail.
- **Durchlassen** — Ermöglicht dem Element den Wechsel in die nächste Scanphase oder zum endgültigen Bestimmungsort.

Primäre Aktionen für die Scans **Auf Anforderung (Standard)** und **Auf Anforderung (Vollständiger Scan)** beinhalten:

- **Element durch Warnung ersetzen** — Ersetzt das Element durch eine Warnmeldung.
- **Nachricht löschen** — Löscht die E-Mail.
- **Durchlassen** — Ermöglicht dem Element den Wechsel in die nächste Scanphase oder zum endgültigen Bestimmungsort.

Sekundäre Aktionen für die Scans **Bei Zugriff** und **Auf Anforderung (Standard)**) beinhalten:

- **Protokollieren** — Die Erkennung wird in einer Berichtsdatei protokolliert.
- **Isolieren** — Eine Kopie des Elements wird in einer Quarantäne-Datenbank gespeichert.
- **Administrator benachrichtigen** — Es wird eine Warnmeldung an den E-Mail-Administrator gesendet.

Sekundäre Aktionen für den Scan **Auf Anforderung (Standard)** beinhalten:

- **Protokollieren** — Die Erkennung wird in einer Berichtsdatei protokolliert.
- **Isolieren** — Eine Kopie des Elements wird in einer Quarantäne-Datenbank gespeichert.
- **Administrator benachrichtigen** — Es wird eine Warnmeldung an den E-Mail-Administrator gesendet.

- **Absender benachrichtigen** — Es wird eine Warnmeldung an den Absender gesendet, wenn die Original-E-Mail nicht aus der Domäne stammt, in der Microsoft® Exchange Server 2003/2007 ausgeführt wird.
- **Empfänger benachrichtigen** — Es wird eine Warnmeldung an den Empfänger gesendet, wenn der Empfänger nicht zu der Domäne gehört, in der Microsoft® Exchange Server 2003/2007 ausgeführt wird.

Geschützter Inhalt

Der Inhalt in einigen E-Mails kann geschützt sein. Er kann dann nicht gescannt werden. Dies gilt z. B. für kennwortgeschützte MS Office-Dateien. Die Richtlinie für geschützten Inhalt legt fest, wie E-Mails mit geschütztem Inhalt bei Erkennung behandelt werden.

1. Wählen Sie unter **Richtlinien-Manager** ein Untermenüelement aus. Die Richtlinienseite für das Untermenüelement wird angezeigt.
2. Wählen Sie die gewünschte Richtlinie aus.
3. Klicken Sie auf **Geschützter Inhalt**. Die Registerkarte **Einstellungen anzeigen** für den Filter für geschützten Inhalt wird angezeigt.
4. Aktivieren oder deaktivieren Sie unter **Aktivierung** das Kontrollkästchen **Aktivieren**, um die Einstellungen für den Filter für geschützten Inhalt für die Richtlinie ein- oder auszuschalten.
5. Zeigen Sie unter **Aktionen** die Aktion an, die bei Erkennung von geschütztem Inhalt durchgeführt werden soll. Klicken Sie zum Ändern dieser Aktionen auf den Link **Bearbeiten**.

Informationen zum Bearbeiten der Aktionen, die bei Erkennung von geschütztem Inhalt durchgeführt werden sollen, finden Sie unter *Primäre und sekundäre Filteraktionen für geschützten Inhalt auf Seite 150*.

Primäre und sekundäre Filteraktionen für geschützten Inhalt

Primäre Aktionen für den Scan **Bei Zugriff** beinhalten:

- **Element durch Warnung ersetzen** — Ersetzt das Element durch eine Warnmeldung.
- **Eingebettetes Element löschen** — Löscht das erkannte Element. Beispielsweise kann eine Anlage gelöscht werden, die eine Erkennungsregel auslöst.
- **Nachricht löschen** — Löscht die E-Mail.
- **Durchlassen** — Ermöglicht dem Element den Wechsel in die nächste Scanphase oder zum endgültigen Bestimmungsort.

Zu den primären Aktionen für die Scans **Auf Anforderung (Standard)**, **Auf Anforderung (Gesperrte Inhalte suchen)**, **Auf Anforderung (Gesperrte Inhalte entfernen)** und**Auf Anforderung (Vollständiger Scan)** zählen Folgende:

- **Element durch Warnung ersetzen** — Ersetzt das Element durch eine Warnmeldung.
- **Nachricht löschen** — Löscht die E-Mail.
- **Durchlassen** — Ermöglicht dem Element den Wechsel in die nächste Scanphase oder zum endgültigen Bestimmungsort.

Sekundäre Aktionen für die Scans **Bei Zugriff**, **Auf Anforderung (Gesperrte Inhalte suchen)** und **Auf Anforderung (Gesperrte Inhalte entfernen)** beinhalten:

- **Protokollieren** — Die Erkennung wird in einer Berichtsdatei protokolliert.
- **Isolieren** — Eine Kopie des Elements wird in einer Quarantäne-Datenbank gespeichert.
- **Administrator benachrichtigen** — Es wird eine Warnmeldung an den E-Mail-Administrator gesendet.

Sekundäre Aktionen für den Scan **Auf Anforderung (Standard)** beinhalten:

- **Protokollieren** — Die Erkennung wird in einer Berichtsdatei protokolliert.
- **Isolieren** — Eine Kopie des Elements wird in einer Quarantäne-Datenbank gespeichert.
- **Administrator benachrichtigen** — Es wird eine Warnmeldung an den E-Mail-Administrator gesendet.
- **Absender benachrichtigen** — Es wird eine Warnmeldung an den Absender gesendet, wenn die Original-E-Mail nicht aus der Domäne stammt, in der Microsoft® Exchange Server 2003/2007 ausgeführt wird.
- **Empfänger benachrichtigen** — Es wird eine Warnmeldung an den Empfänger gesendet, wenn der Empfänger nicht zu der Domäne gehört, in der Microsoft® Exchange Server 2003/2007 ausgeführt wird.

Verschlüsselter Inhalt

Einige E-Mails können verschlüsselt sein. Ihr Inhalt kann nicht gescannt werden. Dies gilt z. B. für alle mit einem Schlüssel verschlüsselten Dateien. Die Richtlinie für verschlüsselten Inhalt legt fest, wie E-Mails mit verschlüsseltem Inhalt bei Erkennung behandelt werden.

1 Wählen Sie unter **Richtlinien-Manager** ein Untermenüelement aus. Die Richtlinienseite für das Untermenüelement wird angezeigt.

2 Wählen Sie die gewünschte Richtlinie aus.

3 Klicken Sie auf **Verschlüsselter Inhalt**. Die Registerkarte **Einstellungen anzeigen** für den Filter für geschützten Inhalt wird angezeigt.

4 Aktivieren oder deaktivieren Sie unter **Aktivierung** das Kontrollkästchen **Aktivieren**, um die Einstellungen für den Filter für verschlüsselten Inhalt für die Richtlinie ein- oder auszuschalten.

5 Zeigen Sie unter **Aktionen** die Aktion an, die bei Erkennung von verschlüsseltem Inhalt durchgeführt werden soll. Klicken Sie zum Ändern dieser Aktionen auf den Link **Bearbeiten**.

Die primären und sekundären Filteraktionen für verschlüsselten Inhalt entsprechen denen für geschützten Inhalt. Weitere Informationen finden Sie unter *Primäre und sekundäre Filteraktionen für geschützten Inhalt auf Seite 150*.

Signierter Inhalt

Beim elektronischen Übertragen oder Hochladen von Daten besteht die Möglichkeit, dass diese versehentlich oder absichtlich geändert werden. Zur Lösung dieses Problems verwenden einige Softwareprogramme digitale Signaturen – die elektronische Form einer handschriftlichen Unterschrift.

Bei einer digitalen Signatur handelt es sich um zusätzliche Informationen, die einer E-Mail hinzugefügt werden, mit denen die Informationen dieser E-Mail identifiziert und authentifiziert werden. Sie ist verschlüsselt und fungiert wie eine eindeutige Zusammenfassung der Informationen, die in der Nachricht mit einem Nachrichten-Digest signiert ist.

Wenn die E-Mail einen Virus oder bösartigen Inhalt enthält oder zu groß ist, säubert oder entfernt die Software u. U. einen Teil der Nachricht. Die E-Mail ist noch gültig und kann gelesen werden, die ursprüngliche digitale Signatur ist jedoch beschädigt. Der Inhalt dieser E-Mail ist nicht vertrauenswürdig, da er möglicherweise auch auf andere Weise geändert wurde. Die Richtlinie für signierte Inhalte gibt an, wie E-Mails mit digitalen Signaturen behandelt werden sollen.

1 Wählen Sie unter **Richtlinien-Manager** ein Untermenüelement aus. Die Richtlinienseite für das Untermenüelement wird angezeigt.

2 Wählen Sie die gewünschte Richtlinie aus.

3 Klicken Sie auf **Signierter Inhalt**. Die Registerkarte **Einstellungen anzeigen** für den Filter für signierten Inhalt wird angezeigt.

4 Aktivieren oder deaktivieren Sie unter **Aktivierung** das Kontrollkästchen **Aktivieren**, um die Einstellungen für den Filter für signierten Inhalt für die Richtlinie ein- oder auszuschalten.

5 Zeigen Sie unter **Aktionen** die Aktion an, die bei Erkennung von signiertem Inhalt durchgeführt werden soll. Klicken Sie zum Ändern dieser Aktionen auf den Link **Bearbeiten**.

Informationen zum Bearbeiten der Aktionen, die bei Erkennung von signiertem Inhalt durchgeführt werden sollen, finden Sie unter *Primäre und sekundäre Filteraktionen für signierten Inhalt auf Seite 153*.

Primäre und sekundäre Filteraktionen für signierten Inhalt

Primäre Aktionen für den Scan **Bei Zugriff** beinhalten:

- **Element durch Warnung ersetzen** — Ersetzt das Element durch eine Warnmeldung.
- **Eingebettetes Element löschen** — Löscht das erkannte Element. Beispielsweise kann eine Anlage gelöscht werden, die eine Erkennungsregel auslöst.
- **Zulassen, dass Änderungen die Signatur zerstören** — Beschädigt die Signatur des signierten Inhalts, wodurch der Inhalt vor dem Hochladen geändert wird.
- **Durchlassen** — Ermöglicht dem Element den Wechsel in die nächste Scanphase oder zum endgültigen Bestimmungsort.

Zu den primären Aktionen für die Scans **Auf Anforderung (Standard)**, **Auf Anforderung (Gesperrte Inhalte suchen)**, **Auf Anforderung (Gesperrte Inhalte entfernen)** und **Auf Anforderung (Vollständiger Scan)** zählen Folgende:

- **Element durch Warnung ersetzen** — Ersetzt das Element durch eine Warnmeldung.
- **Nachricht löschen** — Löscht die E-Mail.
- **Zulassen, dass Änderungen die Signatur zerstören** — Beschädigt die Signatur des signierten Inhalts, wodurch der Inhalt vor dem Hochladen geändert wird.
- **Durchlassen** — Ermöglicht dem Element den Wechsel in die nächste Scanphase oder zum endgültigen Bestimmungsort.

Sekundäre Aktionen für die Scans **Bei Zugriff**, **Auf Anforderung (Standard)**, **Auf Anforderung (Gesperrte Inhalte suchen)**, **Auf Anforderung (Gesperrte Inhalte entfernen)** und **Auf Anforderung (Vollständiger Scan)** beinhalten:

- **Protokollieren** — Die Erkennung wird in einer Berichtsdatei protokolliert.
- **Isolieren** — Eine Kopie des Elements wird in einer Quarantäne-Datenbank gespeichert.
- **Administrator benachrichtigen** — Es wird eine Warnmeldung an den E-Mail-Administrator gesendet.
- **Absender benachrichtigen** — Es wird eine Warnmeldung an den Absender gesendet, wenn die Original-E-Mail nicht aus der Domäne stammt, in der Microsoft® Exchange Server 2003/2007 ausgeführt wird.
- **Empfänger benachrichtigen** — Es wird eine Warnmeldung an den Empfänger gesendet, wenn der Empfänger nicht zu der Domäne gehört, in der Microsoft® Exchange Server 2003/2007 ausgeführt wird.

Kennwortgeschützte Dateien

Kennwortgeschützte Dateien lassen sich nicht scannen. Dies gilt z. B. für RAR- oder ZIP-Dateien. Die Richtlinie für kennwortgeschützte Dateien legt fest, wie E-Mails mit kennwortgeschütztem Inhalt bei der Erkennung behandelt werden.

1. Wählen Sie unter **Richtlinien-Manager** ein Untermenüelement aus. Die Richtlinienseite für das Untermenüelement wird angezeigt.
2. Wählen Sie die gewünschte Richtlinie aus.
3. Klicken Sie auf **Kennwortgeschützte Dateien**. Die Registerkarte **Einstellungen anzeigen** für den Filter für kennwortgeschützte Dateien wird angezeigt.
4. Aktivieren oder deaktivieren Sie unter **Aktivierung** das Kontrollkästchen **Aktivieren**, um die Einstellungen für den Filter für kennwortgeschützte Dateien für die Richtlinie ein- oder auszuschalten.
5. Zeigen Sie unter **Aktionen** die Aktion an, die bei Erkennung von kennwortgeschütztem Inhalt durchgeführt werden soll. Klicken Sie zum Ändern dieser Aktionen auf den Link **Bearbeiten**.

Informationen zum Bearbeiten der Aktionen, die bei Erkennung von kennwortgeschütztem Inhalt durchgeführt werden sollen, finden Sie unter *Primäre und sekundäre Aktionen für kennwortgeschützten Inhalt auf Seite 155*.

Primäre und sekundäre Aktionen für kennwortgeschützten Inhalt

Primäre Aktionen für den Scan **Bei Zugriff** beinhalten:

- **Element durch Warnung ersetzen** — Ersetzt das erkannte Element durch eine Warnmeldung.
- **Nachricht löschen** — Löscht die E-Mail.
- **Eingebettetes Element löschen** — Löscht das erkannte Element. Beispielsweise kann eine Anlage gelöscht werden, die eine Erkennungsregel auslöst.
- **Durchlassen** — Ermöglicht dem Element den Wechsel in die nächste Scanphase oder zum endgültigen Bestimmungsort.

Zu den primären Aktionen für die Scans **Auf Anforderung (Standard)**, **Auf Anforderung (Gesperrte Inhalte suchen)**, **Auf Anforderung (Gesperrte Inhalte entfernen)** und **Auf Anforderung (Vollständiger Scan)** zählen Folgende:

- **Element durch Warnung ersetzen** — Ersetzt das erkannte Element durch eine Warnmeldung.
- **Nachricht löschen** — Löscht die E-Mail.
- **Durchlassen** — Ermöglicht dem Element den Wechsel in die nächste Scanphase oder zum endgültigen Bestimmungsort.

Die sekundären Aktionen für die Scans **Bei Zugriff**, **Auf Anforderung (Gesperrte Inhalte suchen)**, **Auf Anforderung (Gesperrte Inhalte entfernen)** und **Auf Anforderung (Vollständiger Scan)** beinhalten:

- **Protokollieren** — Die Erkennung wird in einer Berichtsdatei protokolliert.
- **Isolieren** — Eine Kopie des Elements wird in einer Quarantäne-Datenbank gespeichert.
- **Administrator benachrichtigen** — Es wird eine Warnmeldung an den E-Mail-Administrator gesendet.

Sekundäre Aktionen für den Scan **Auf Anforderung (Standard)** beinhalten:

- **Protokollieren** — Die Erkennung wird in einer Berichtsdatei protokolliert.
- **Isolieren** — Eine Kopie des Elements wird in einer Quarantäne-Datenbank gespeichert.

- **Administrator benachrichtigen** — Es wird eine Warnmeldung an den E-Mail-Administrator gesendet.
- **Absender benachrichtigen** — Es wird eine Warnmeldung an den Absender gesendet, wenn die Original-E-Mail nicht aus der Domäne stammt, in der Microsoft® Exchange Server 2003/2007 ausgeführt wird.
- **Empfänger benachrichtigen** — Es wird eine Warnmeldung an den Empfänger gesendet, wenn der Empfänger nicht zu der Domäne gehört, in der Microsoft® Exchange Server 2003/2007 ausgeführt wird.

Scannersteuerung

Mithilfe der Einstellungen für die **Scannersteuerung** können Sie Verschachtelungsebene, Dateigröße oder die zulässige Scandauer für das Scannen von E-Mails angeben.

1. Wählen Sie unter **Richtlinien-Manager** ein Untermenüelement aus. Die Richtlinienseite für das Untermenüelement wird angezeigt.
2. Wählen Sie die gewünschte Richtlinie aus.
3. Klicken Sie auf **Scannersteuerung**. Die Registerkarte **Einstellungen anzeigen** für den Filter für Scannersteuerung wird angezeigt.
4. Aktivieren oder deaktivieren Sie unter **Aktivierung** das Kontrollkästchen **Aktivieren**, um die Einstellungen für den Filter für kennwortgeschützte Dateien für die Richtlinie ein- oder auszuschalten.
5. Wählen Sie unter **Optionen** den Optionssatz für die Scannersteuerung aus, den Sie anzeigen oder konfigurieren möchten. Sie haben folgende Möglichkeiten:
   - **Kerneinstellungen für Scannersteuerung** — Zeigt eine Übersicht des Optionssatzes für die Scannersteuerung an, der standardmäßig verwendet wird, wenn keine alternativen Optionssätze für die Scannersteuerung verfügbar sind.
   - **Neuen Optionssatz erstellen** — Ermöglicht die Erstellung eines neuen Optionssatzes für diese Richtlinie.

Schrittweise Anleitungen finden Sie unter *Erstellen eines neuen Optionssatzes für Einstellungen der Scannersteuerung auf Seite 157*.

   - **Bearbeiten** — Ermöglicht die Bearbeitung des ausgewählten Optionssatzes.

6 Wählen Sie unter **Warnungsauswahl** eine vorhandene Warnung aus, die bei Auslösen einer Scannersteuerungsoption verwendet wird, oder klicken Sie zum Erstellen einer neuen Warnung auf **Erstellen**.
Wenn der Text der Warnmeldung nicht angezeigt wird, Sie ihn jedoch in einer Vorschau anzeigen möchten, klicken Sie auf **Anzeigen/Ausblenden**, um den Text anzuzeigen. Wenn der Text der Warnmeldung angezeigt wird, klicken Sie auf **Anzeigen/Ausblenden**, um ihn auszublenden.

Weitere Informationen hierzu finden Sie unter *Erstellen einer neuen Warnung auf Seite 133*.

7 Zeigen Sie unter **Aktionen** die Aktionen an, die bei Überschreiten der Verschachtelungsebene, Dateigröße oder Scanzeit durchgeführt werden sollen, oder bearbeiten Sie die Aktionen Klicken Sie zum Ändern dieser Aktionen auf **Bearbeiten**.

Weitere Informationen hierzu finden Sie unter *Bearbeiten von primären und sekundären Scannersteuerungsaktionen auf Seite 158*.

Erstellen eines neuen Optionssatzes für Einstellungen der Scannersteuerung

1 Wählen Sie unter **Richtlinien-Manager** ein Untermenüelement aus. Die Richtlinienseite für das Untermenüelement wird angezeigt.

2 Wählen Sie die gewünschte Richtlinie aus.

3 Klicken Sie auf **Scannersteuerung**. Die Registerkarte **Einstellungen anzeigen** für den Filter für Scannersteuerung wird angezeigt.

4 Klicken Sie im Dropdown-Menü **Optionen** auf **neuen Optionssatz erstellen**. Die Seite **Scannersteuerung** wird angezeigt.

5 Geben Sie unter **Instanzname** einen Instanznamen für die Einstellungen der Scannersteuerung ein. Dieses Feld muss ausgefüllt werden.

6 Geben Sie unter **Maximale Verschachtelungsebene** die Ebene an, bis zu der der Scanner scannen soll, wenn eine Anlage komprimierte Dateien enthält, die weitere komprimierte Dateien enthalten. Empfehlenswert ist die Begrenzung auf eine Scantiefe von 100.

7 Geben Sie unter **Maximale dekomprimierte Dateigröße (MB)** die maximal zulässige Größe einer Datei (in MB) an, wenn sie zum Scannen dekomprimiert wird. Empfehlenswert ist die Begrenzung auf maximal 100 MB.

8 Geben Sie unter **Maximale Scanzeit (Minuten)** den maximalen Zeitbereich für das Scannen von Dateien in Minuten ein. Empfehlenswert ist die Begrenzung auf eine Dauer von maximal 10 Minuten.

9 Klicken Sie auf **Speichern** und dann auf **Übernehmen**.

Bearbeiten von primären und sekundären Scannersteuerungsaktionen

Unter **Scannersteuerungsaktionen** können Sie die Aktionen angeben, die unter folgenden Bedingungen ausgeführt werden:

- Die maximale Verschachtelungstiefe ist überschritten.
- Die maximale Dateigröße ist überschritten.
- Die maximale Scanzeit ist überschritten.

Primäre Aktionen für den Scan **Bei Zugriff** beinhalten:

- **Erkanntes Element durch Warnung ersetzen** — Ersetzt ein erkanntes Element, z. B. einen Anhang, durch eine Warnmeldung.
- **Eingebettetes Element löschen** — Löscht das erkannte Element. Beispielsweise kann eine Anlage gelöscht werden, die eine Erkennungsregel auslöst.
- **Nachricht löschen** — Löscht die E-Mail.
- **Durchlassen** — Ermöglicht dem Element den Wechsel in die nächste Scanphase oder zum endgültigen Bestimmungsort.

Zu den primären Aktionen für die Scans **Auf Anforderung (Standard)**, **Auf Anforderung (Viren suchen)**, **Auf Anforderung (Viren entfernen)**, **Auf Anforderung (Gesperrte Inhalte suchen)**, **Auf Anforderung (Gesperrte Inhalte entfernen)**, **Auf Anforderung (Vollständiger Scan)** und **Gateway** zählen Folgende:

- **Erkanntes Element durch Warnung ersetzen** — Ersetzt ein erkanntes Element, z. B. einen Anhang, durch eine Warnmeldung.
- **Nachricht löschen** — Löscht die E-Mail.
- **Durchlassen** — Ermöglicht dem Element den Wechsel in die nächste Scanphase oder zum endgültigen Bestimmungsort.

Sekundäre Aktionen für die Scans **Bei Zugriff** und **Auf Anforderung (Standard)**) beinhalten:

- **Protokollieren** — Die Erkennung wird in einer Berichtsdatei protokolliert.
- **Isolieren** — Eine Kopie des Elements wird in einer Quarantäne-Datenbank gespeichert.
- **Administrator benachrichtigen** — Es wird eine Warnmeldung an den E-Mail-Administrator gesendet.

- **Absender benachrichtigen** — Es wird eine Warnmeldung an den Absender gesendet, wenn die Original-E-Mail nicht aus der Domäne stammt, in der Microsoft® Exchange Server 2003/2007 ausgeführt wird.
- **Empfänger benachrichtigen** — Es wird eine Warnmeldung an den Empfänger gesendet, wenn der Empfänger nicht zu der Domäne gehört, in der Microsoft® Exchange Server 2003/2007 ausgeführt wird.

Sekundäre Aktionen für die Scans **Auf Anforderung (Viren suchen)**, **Auf Anforderung (Viren entfernen)**, **Auf Anforderung (Gesperrte Inhalte suchen)**, **Auf Anforderung (Gesperrte Inhalte entfernen)**, **Auf Anforderung (Vollständiger Scan)** und **Gateway** zählen Folgende:

- **Protokollieren** — Die Erkennung wird in einer Berichtsdatei protokolliert.
- **Isolieren** — Eine Kopie des Elements wird in einer Quarantäne-Datenbank gespeichert.
- **Administrator benachrichtigen** — Es wird eine Warnmeldung an den E-Mail-Administrator gesendet.

Einstellungen für MIME-Nachrichten

Die Einstellungen für MIME-Nachrichten legen die Verarbeitung von MIME-Nachrichten fest.

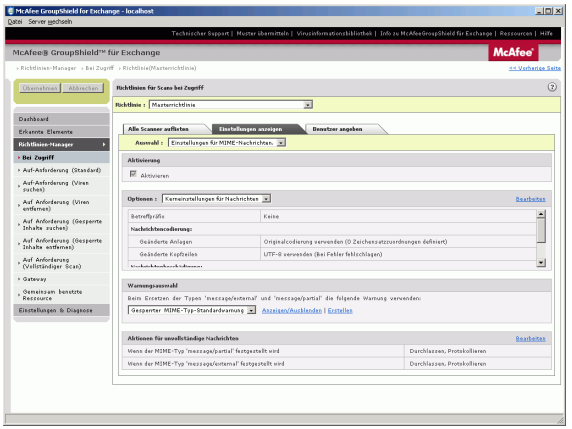
MIME (Multipurpose Internet Mail Extensions) ist ein Kommunikationsstandard, der die Übertragung von Nicht-ASCII-Formaten über Protokolle gestattet, die nur 7-Bit-ASCII-Zeichen unterstützen.

Die Einstellungen für MIME-Nachrichten sind Standardeinstellungen und können nur von fortgeschrittenen Benutzern geändert werden.

1. Wählen Sie unter **Richtlinien-Manager** ein Untermenüelement aus. Die Richtlinienseite für das Untermenüelement wird angezeigt.
2. Wählen Sie die gewünschte Richtlinie aus.

3 Klicken Sie auf **Einstellungen für MIME-Nachrichten**. Die Registerkarte **Einstellungen anzeigen** für die Einstellungen für MIME-Nachrichten wird angezeigt.

Abbildung 10-2 Einstellungen für MIME-Nachrichten



4 Aktivieren oder deaktivieren Sie unter **Aktivierung** das Kontrollkästchen **Aktivieren**, um die Einstellungen der MIME-Nachrichten für die Richtlinie ein- oder auszuschalten.

5 Wählen Sie unter **Optionen** eine der folgenden Optionen aus:

- **Kerneinstellungen für Nachrichten** — Ermöglicht die Anzeige und Konfiguration der Standardeinstellungen des Nachrichtengrößenfilters.
- Eine vorhandene Instanz der MIME-Nachrichteneinstellung.
- **neuen Optionssatz erstellen** — Ermöglicht das Erstellen eines neuen Optionssatzes der MIME-Nachrichteneinstellungen für eine ausgewählte Richtlinie.

Weitere Informationen hierzu finden Sie unter *Erstellen eines neuen Optionssatzes für MIME-Nachrichteneinstellungen auf Seite 161*.

- **Bearbeiten** — Ermöglicht die Änderung der Optionen von MIME-Nachrichteneinstellungen, die mit einer Richtlinie verknüpft sind.

6 Wählen Sie unter **Warnungsauswahl** die Option **Standardwarnung für gesperrten MIME-Typ** oder eine vorhandene Warnung aus der Dropdown-Liste. Oder klicken Sie zum Erstellen einer neuen Warnung auf **Erstellen**.

Weitere Informationen hierzu finden Sie unter *Erstellen einer neuen Warnung auf Seite 133*.

7 Zeigen Sie unter **Aktionen für unvollständige Nachrichten** die Aktionen an, die bei Erkennung von Partial-MIME- oder External-MIME-Nachrichten angezeigt oder bearbeitet werden. Klicken Sie zum Ändern dieser Aktionen auf **Bearbeiten**.

Weitere Informationen hierzu finden Sie unter *Primäre und sekundäre Aktionen für unvollständige Nachrichten auf Seite 163*.

Erstellen eines neuen Optionssatzes für MIME-Nachrichteneinstellungen

1 Wählen Sie unter **Richtlinien-Manager** ein Untermenüelement aus. Die Richtlinienseite für das Untermenüelement wird angezeigt.

2 Wählen Sie die gewünschte Richtlinie aus.

3 Klicken Sie auf **Einstellungen für MIME-Nachrichten**. Die Registerkarte **Einstellungen anzeigen** für die MIME-Nachrichteneinstellungen wird angezeigt.

4 Klicken Sie im Dropdown-Menü **Optionen** auf **neuen Optionssatz erstellen**. Die Seite **Nachrichteneinstellungen** wird mit vier Registerkarten angezeigt: **Optionen**, **Erweitert**, **MIME-Typen** und **Zeichensätze**.

5 Geben Sie unter **Instanzname** einen Instanznamen für die MIME-Nachrichteneinstellungen an. Dieses Feld muss ausgefüllt werden.

6 Geben Sie auf der Registerkarte **Optionen** unter **Präfix für Nachrichtenbetreff** ein Präfix ein.

7 Wählen Sie unter **Bevorzugte Neucodierung von Anlagen in einer MIME-Nachricht** eine Neucodierungsmethode aus, die für die Neucodierung von Anlagen in MIME-Nachrichten verwendet wird.

- **Neucodierung mit ursprünglicher Nachrichtencodierung**
- **Neucodierung mit HTML und numerischen Unicodeverweisen**
- **Neucodierung mit dem folgenden Zeichensatz** (In diesem Fall wählen Sie einen Zeichensatz aus der Dropdown-Liste aus.)

8 Wählen Sie unter **Bevorzugte Neucodierung von geänderten Betreffkopfzeilen** eine Neucodierungsmethode aus, die für die Neucodierung von Betreffkopfzeilen in MIME-Nachrichten verwendet wird.

- **Neucodierung mit UTF-8**
- **Neucodierung mit ursprünglichem Codierungsschema**
- **Neucodierung mit dem folgenden Zeichensatz** (In diesem Fall wählen Sie einen Zeichensatz aus der Dropdown-Liste aus.)

9 Wählen Sie eine der folgenden Optionen aus, wenn die Neucodierung einer Betreffkopfzeile fehlschlägt:

- **Als Fehler behandeln** — Die MIME-Nachricht wird abgewiesen.
- **UTF-8 verwenden** — Die MIME-Nachricht wird in UTF-8 codiert.

Sie können Schritt 9 nur durchführen, wenn Sie unter **Bevorzugte Neucodierung von geänderten Betreffkopfzeilen** die Option **Neucodierung mit ursprünglichem Codierungsschema** oder **Neucodierung mit dem folgenden Zeichensatz** auswählen.

10 Wählen Sie auf der Registerkarte **Erweitert** eine der folgenden Codierungsmethoden aus, die für den Textteil einer E-Mail verwendet werden soll:

- **Quoted-Printable** — Eignet sich ideal für Nachrichten mit hauptsächlich ASCII-Zeichen.
- **Base64** — Hat einen festen Overhead und eignet sich ideal für Nichttextdaten und Nachrichten mit wenig ASCII-Text.
- **8-Bit** — Ideal für SMTP-Server, die die 8BITMIME-Transport-SMTP-Erweiterung unterstützen.

11 Wählen Sie die Option **7-Bit-Text nicht codieren** aus, oder heben Sie die Auswahl auf.

12 Wählen Sie unter **Standardzeichensatz für Decodierung** den Zeichensatz aus, der für die Decodierung verwendet werden soll, wenn keiner in der MIME-Kopfzeile angegeben ist.

13 Geben Sie unter **Maximale Anzahl von MIME-Bestandteilen** die maximale Anzahl von MIME-Bestandteilen an, die in einer MIME-Nachricht enthalten sein können. Der Standardwert liegt bei 10000 MIME-Bestandteilen.

14 Wählen Sie unter **Kopfzeilenbeschädigung in einer MIME-Nachricht** die gewünschte Option:

- **Als beschädigten Inhalt behandeln und entsprechende Aktion durchführen**
- **Nicht als beschädigten Inhalt behandeln**

15 Wählen Sie unter **NULL-Zeichen in den Kopfzeilen einer MIME-Nachricht** die gewünschte Option:

- **Als beschädigten Inhalt behandeln und entsprechende Aktion durchführen**
- **Nicht als beschädigten Inhalt behandeln**

16 Geben Sie auf der Registerkarte **MIME-Typen** an, welche MIME-Typen als Textanlagen und welche als Binäranlagen behandelt werden sollen.

Klicken Sie auf **Hinzufügen**, um die MIME-Typen der Liste hinzuzufügen, oder auf **Löschen**, um einen MIME-Typ aus der Liste zu löschen. Doppelte Einträge sind nicht zulässig.

17 Wählen Sie auf der Registerkarte **Zeichensätze** einen Zeichensatz und entsprechende Alternativen aus. Deaktivieren Sie das Kontrollkästchen **Fest**, und klicken Sie auf **Hinzufügen**, um eine alternative Zeichensatzzuordnung zu dem in der MIME-Nachricht angegebenen Zeichensatz anzugeben.

Klicken Sie zum Bearbeiten von Zeichenzuordnungen auf **Bearbeiten**, zum Löschen von Zeichenzuordnungen auf **Löschen** und zum Speichern von Änderungen an Zeichenzuordnungen auf **Speichern**.

Die Option **Speichern** steht nur zur Verfügung, wenn Sie auf **Bearbeiten** klicken.

18 Klicken Sie auf **Speichern** und dann auf **Übernehmen**.

Primäre und sekundäre Aktionen für unvollständige Nachrichten

Zu den primären Aktionen für die Scans **Bei Zugriff**, **Auf Anforderung (Standard)**, **Auf Anforderung (Viren suchen)**, **Auf Anforderung (Viren entfernen)**, **Auf Anforderung (Gesperrte Inhalte suchen)**, **Auf Anforderung (Gesperrte Inhalte entfernen)**, **Auf Anforderung (Vollständiger Scan)** und **Gateway** zählen Folgende:

- **Durchlassen** — Die MIME-Nachricht wird bis zum eigentlichen Zielpunkt durchgelassen.
- **Nachricht löschen** — Die MIME-Nachricht wird gelöscht.
- **Nachricht durch Warnung ersetzen** — Die MIME-Nachricht wird durch eine Warnmeldung ersetzt.

Sekundäre Aktionen für den Scan **Bei Zugriff** beinhalten:

- **Protokollieren** — Die Erkennung wird in einer Berichtsdatei protokolliert.
- **Isolieren** — Eine Kopie des Elements wird in einer Quarantäne-Datenbank gespeichert.
- **Administrator benachrichtigen** — Es wird eine Warnmeldung an den E-Mail-Administrator gesendet.
- **Absender benachrichtigen** — Es wird eine Warnmeldung an den Absender gesendet, wenn die Original-E-Mail nicht aus der Domäne stammt, in der Microsoft® Exchange Server 2003/2007 ausgeführt wird.

- **Empfänger benachrichtigen** — Es wird eine Warnmeldung an den Empfänger gesendet, wenn der Empfänger nicht zu der Domäne gehört, in der Microsoft® Exchange Server 2003/2007 ausgeführt wird.

Die sekundären Aktionen für den Scan **Auf Anforderung (Standard)** umfassen zwei zusätzliche primäre Aktionen:

- **Absender benachrichtigen** — Es wird eine Warnmeldung an den internen Absender gesendet, wenn die Original-E-Mail aus der Domäne stammt, in der Microsoft® Exchange Server 2003/2007 ausgeführt wird.
- **Empfänger benachrichtigen** — Es wird eine Warnmeldung an den Empfänger gesendet, wenn der Empfänger zu der Domäne gehört, in der Microsoft® Exchange Server 2003/2007 ausgeführt wird.

Sekundäre Aktionen für die Scans **Auf Anforderung (Gesperrte Inhalte suchen)**, **Auf Anforderung (Gesperrte Inhalte entfernen)**, **Auf Anforderung (Vollständiger Scan)** und **Gateway** beinhalten:

Protokollieren — Die Erkennung wird in einer Berichtsdatei protokolliert.

Isolieren — Eine Kopie des Elements wird in einer Quarantäne-Datenbank gespeichert.

Administrator benachrichtigen — Es wird eine Warnmeldung an den E-Mail-Administrator gesendet.

HTML-Dateien

1. Wählen Sie unter **Richtlinien-Manager** ein Untermenüelement aus. Die Richtlinienseite für das Untermenüelement wird angezeigt.
2. Wählen Sie die gewünschte Richtlinie aus.
3. Klicken Sie auf **HTML-Dateien**. Die Registerkarte **Einstellungen anzeigen** für HTML-Dateien wird angezeigt.
4. Aktivieren oder deaktivieren Sie unter **Aktivierung** das Kontrollkästchen **Aktivieren**, um die HTML-Dateieinstellungen für die Richtlinie ein- oder auszuschalten.
5. Wählen Sie unter **Optionen** eine der folgenden Optionen aus:
   - **Standardeinstellungen für HTML** — Ermöglicht die Anzeige und Konfiguration der Standardeinstellungen für HTML-Dateien.
   - Eine vorhandene Instanz der HTML-Dateieinstellungen.

- **neuen Optionssatz erstellen** — Ermöglicht das Erstellen eines neuen Optionssatzes der HTML-Dateieinstellungen für eine ausgewählte Richtlinie.

Weitere Informationen hierzu finden Sie unter *Erstellen eines neuen Optionssatzes für HTML-Dateieinstellungen auf Seite 165*.

- **Bearbeiten** — Ermöglicht die Änderung der Optionen von HTML-Dateieinstellungen, die mit einer Richtlinie verknüpft sind.

Erstellen eines neuen Optionssatzes für HTML-Dateieinstellungen

1. Wählen Sie unter **Richtlinien-Manager** ein Untermenüelement aus. Die Richtlinienseite für das Untermenüelement wird angezeigt.
2. Wählen Sie die gewünschte Richtlinie aus.
3. Klicken Sie auf **HTML-Dateien**. Die Registerkarte **Einstellungen anzeigen** für HTML-Dateieinstellungen wird angezeigt.
4. Klicken Sie im Dropdown-Menü **Optionen** auf **neuen Optionssatz erstellen**. Die Seite **HTML-Dateien** wird angezeigt.
5. Geben Sie unter **Instanzname** einen Instanznamen für die HTML-Dateieinstellungen an. Dieses Feld muss ausgefüllt werden.
6. Unter **Die folgenden Elemente scannen** stehen folgende Optionen zur Auswahl:

   - **Kommentare** — HTML-Nachrichten werden nach Kommentarelementen gescannt.
     Beispiel: `<!-- Kommentartext --!>`
   - **Metadaten** — HTML-Nachrichten werden nach Metadatenelementen gescannt.
     Beispiel: `< META EQUI="Expires" Content="Tue, 04 June 2007 21:29:02">`
   - **Link-URLs ("<a href=...")** — HTML-Nachrichten werden nach URL-Elementen gescannt.
     Beispiel: `<a HREF="McAfee.htm">`
   - **Quell-URLs ("<img src=...")** — HTML-Nachrichten werden nach Quell-URL-Elementen gescannt.
     Beispiel:
     `<IMG SRC="..\..\images\icons\mcafee_logo_rotating75.gif">`
   - **JavaScript/VBScript** — HTML-Nachrichten werden nach JavaScript- oder Visual Basic-Skripten gescannt.
     Beispiel: `<script language="javascript" scr="mfe/mfe.js">`

7 Unter **Die folgenden ausführbaren Elemente entfernen** stehen folgende Optionen zur Auswahl:

- **JavaScript/VBScript** — JavaScript- oder Visual Basic-Skripte werden aus HTML-Nachrichten zu entfernt.
  Beispiel: `<script language="javascript" scr="mfe/mfe.js">`
- **Java-Applets** — Java-Applet-Elemente werden aus HTML-Nachrichten entfernt.
  Beispiel: `<APPLET code="XYZApp.class" codebase="HTML ....." ></APPLET>`
- **ActiveX-Steuerelemente** — ActiveX-Steuerelemente werden aus HTML-Nachrichten zu entfernt.
  Beispiel: `<OBJECT ID="clock" data="http://www.mcafee.com/vscan.png" type="image/png"> VirusScan Image </OBJECT>`
- **Macromedia Flash** — Macromedia Flash-Elemente werden aus HTML-Nachrichten entfernt. Diese Option ist aktiviert, wenn Sie ActiveX-Steuerelemente ausgewählt haben.
  Beispiel: `<EMBED SCR="somefilename.swf" width="500" height="200">`

8 Klicken Sie auf **Speichern** und dann auf **Übernehmen**.

Nachrichtengrößenfilterung

1 Wählen Sie unter **Richtlinien-Manager** die Option **Gateway**. Die Richtlinienseite für **Gateway** wird angezeigt.

2 Wählen Sie die gewünschte Richtlinie aus.

3 Klicken Sie auf **Nachrichtengrößenfilterung**. Die Registerkarte **Einstellungen anzeigen** für die Nachrichtengrößenfilterung wird angezeigt.

4 Aktivieren oder deaktivieren Sie unter **Aktivierung** das Kontrollkästchen **Aktivieren**, um die Einstellungen des Nachrichtengrößenfilters für die Richtlinie ein- oder auszuschalten.

5 Wählen Sie unter **Optionen** eine der folgenden Optionen aus:

- **Standardeinstellungen** — Ermöglicht die Anzeige und Konfiguration der Standardeinstellungen des Nachrichtengrößenfilters.
- Eine vorhandenen Instanz der Einstellungen für des Nachrichtengrößenfilters.
- **neuen Optionssatz erstellen** — Ermöglicht das Erstellen eines neuen Optionssatzes der Einstellungen des Nachrichtengrößenfilters für eine ausgewählte Richtlinie.

Weitere Informationen hierzu finden Sie unter *Erstellen eines neuen Optionssatzes für den Nachrichtengrößenfilter auf Seite 167*.

- **Bearbeiten** — Ermöglicht die Änderung der Optionen der Einstellungen für den Nachrichtengrößenfilter, die mit einer Richtlinie verknüpft sind.

6 Unter **Aktionen** zeigen Sie die Aktionen für die Nachrichtengrößenfilterung an oder bearbeiten diese.

Weitere Informationen hierzu finden Sie unter *Primäre und sekundäre Aktionen für die Nachrichtengrößenfilterung auf Seite 168*.

Erstellen eines neuen Optionssatzes für den Nachrichtengrößenfilter

1 Wählen Sie unter **Richtlinien-Manager** die Option **Gateway**. Die Richtlinienseite für **Gateway** wird angezeigt.

2 Wählen Sie die gewünschte Richtlinie aus.

3 Klicken Sie auf **Nachrichtengrößenfilterung**. Die Registerkarte **Einstellungen anzeigen** für die Nachrichtengrößenfilterung wird angezeigt.

4 Klicken Sie im Dropdown-Menü **Optionen** auf **neuen Optionssatz erstellen**. Die Seite **Nachrichtengrößenfilterung** wird angezeigt.

5 Geben Sie unter **Instanzname** einen Instanznamen für die Einstellungen des Nachrichtengrößenfilters ein. Dieses Feld muss ausgefüllt werden.

6 Geben Sie unter **Maximale Gesamtnachrichtengröße (KB)** die maximal zulässige Größe einer E-Mail (in KB) ein. Die empfohlene Größe liegt bei 100.000 KB (100 MB).

7 Geben Sie unter **Maximale Anlagengröße (KB)** die maximal zulässige Größe einer E-Mail-Anlage (in KB) ein. Es wird eine Größe von 32.000 KB empfohlen.

8 Geben Sie unter **Maximale Anzahl von Anlagen** die maximal zulässige Anzahl an Anlagen ein, die eine E-Mail haben darf. Es sollten nicht mehr als 500 Anlagen festgelegt werden.

9 Klicken Sie auf **Speichern** und dann auf **Übernehmen**.

Die Nachrichtengrößenfilterung wird sowohl auf eingehende als auch auf ausgehende E-Mails angewendet.

Primäre und sekundäre Aktionen für die Nachrichtengrößenfilterung

Primäre Aktionen auf der Registerkarte **Nachrichtengröße** beinhalten:

- **Alle Anlagen durch eine einzige Warnung ersetzen** — Erstellt für alle Anlagen eine einzelne Warnmeldung und ersetzt alle Anlagen durch diese, anstatt eine Warnmeldung für jede Anlage in einer E-Mail zu erstellen.
- **Durchlassen** — Ermöglicht dem Element den Wechsel in die nächste Scanphase oder zum endgültigen Bestimmungsort.

Primäre Aktionen auf der Registerkarte **Anlagengröße** beinhalten:

- **Anlage durch Warnung ersetzen** — Ersetzt die Anlage durch eine Warnmeldung. In diesem Fall erfolgt eine Warnung für jede Anlage, die eine Erkennung auslöst.
- **Anlage entfernen** — Entfernt die Anlage von der E-Mail.
- **Durchlassen** — Ermöglicht dem Element den Wechsel in die nächste Scanphase oder zum endgültigen Bestimmungsort.

Primäre Aktionen auf der Registerkarte **Anlagenzahl** beinhalten:

- **Alle Anlagen durch eine einzige Warnung ersetzen** — Erstellt für alle Anlagen eine einzelne Warnmeldung und ersetzt alle Anlagen durch diese, anstatt eine Warnmeldung für jede Anlage in einer E-Mail zu erstellen.
- **Alle Anlagen entfernen** — Entfernt alle Anlagen von der E-Mail.
- **Durchlassen** — Ermöglicht dem Element den Wechsel in die nächste Scanphase oder zum endgültigen Bestimmungsort.

Sekundäre Aktionen sind auf allen Registerkarten gleich.

- **Protokollieren** — Die Erkennung wird in einer Berichtsdatei protokolliert.
- **Isolieren** — Eine Kopie des Elements wird in einer Quarantäne-Datenbank gespeichert.
- **Administrator benachrichtigen** — Es wird eine Warnmeldung an den E-Mail-Administrator gesendet.
- **Absender benachrichtigen** — Es wird eine Warnmeldung an den Absender gesendet, wenn die Original-E-Mail nicht aus der Domäne stammt, in der Microsoft® Exchange Server 2003/2007 ausgeführt wird.
- **Empfänger benachrichtigen** — Es wird eine Warnmeldung an den Empfänger gesendet, wenn der Empfänger nicht zu der Domäne gehört, in der Microsoft® Exchange Server 2003/2007 ausgeführt wird.

Verschiedenes

Zu diesen Einstellungen gehören:

- **Warneinstellungen**
- **Text für Haftungsausschluss**

Warneinstellungen

Warnmeldungen dienen zur Benachrichtigung bei Eintreten eines bestimmten Ereignisses. Mit **Warneinstellungen** können Sie zusätzliche Informationen für diese Warnungen festlegen.

1. Wählen Sie unter **Richtlinien-Manager** ein Untermenüelement aus. Die Richtlinienseite für das Untermenüelement wird angezeigt.
2. Wählen Sie die gewünschte Richtlinie aus.
3. Klicken Sie auf **Warneinstellungen**. Die Registerkarte **Einstellungen anzeigen** für Warneinstellungen wird angezeigt.
4. Aktivieren oder deaktivieren Sie unter **Aktivierung** das Kontrollkästchen **Aktivieren**, um die Warneinstellungen für die Richtlinie ein- oder auszuschalten.
5. Wählen Sie unter **Optionen** eine der folgenden Optionen aus:
   - **Einstellungen für Standardwarnung** — Ermöglicht die Anzeige und Konfiguration der Einstellungen für die Standardwarnung.
   - Eine vorhandene Warnung.
   - **neuen Optionssatz erstellen** — Ermöglicht das Erstellen eines neuen Optionssatzes der Warneinstellungen für eine ausgewählte Richtlinie.

Weitere Informationen hierzu finden Sie unter *Erstellen eines neuen Optionssatzes für Warneinstellungen auf Seite 170*.

   - **Bearbeiten** — Ermöglicht die Änderung der Optionen von Warneinstellungen, die mit einer Richtlinie verknüpft sind.

Erstellen eines neuen Optionssatzes für Warneinstellungen

1 Wählen Sie unter **Richtlinien-Manager** ein Untermenüelement aus. Die Richtlinienseite für das Untermenüelement wird angezeigt.

2 Wählen Sie die gewünschte Richtlinie aus.

3 Klicken Sie auf **Warneinstellungen**. Die Registerkarte **Einstellungen anzeigen** für Warneinstellungen wird angezeigt.

4 Klicken Sie im Dropdown-Menü **Optionen** auf **neuen Optionssatz erstellen**. Die Seite **Warneinstellungen** wird angezeigt.

5 Geben Sie unter **Instanzname** einen Instanznamen für die Warneinstellungen an. Dieses Feld muss ausgefüllt werden.

6 Wählen Sie **HTML** oder **Einfacher Text** als **Warnformat**.

7 Wählen Sie im Dropdown-Menü **Zeichencodierung** den gewünschten Zeichensatz.

8 Geben Sie unter **Warndateiname** den Dateinamen für diese Warnung ein sowie die entsprechende Dateierweiterung für HTML (.htm) oder Nur-Text (.txt).

9 Aktivieren oder deaktivieren Sie **Kopfzeilen für Warnung aktivieren**, um die Verwendung von Warnungskopfzeilen zu ermöglichen.

10 Geben Sie in das Texteingabefeld **Warnungskopfzeile** die Kopfzeile für die Warnung ein.

11 Wählen Sie unter **Anzeigen** die Option **HTML-Inhalt (WYSIWYG)** oder **HTML-Inhalt (Quelle)** aus, je nachdem, ob der HTML-Text in der **Warnungskopfzeile** als kompilierter Code oder Quellcode angezeigt werden soll.

Die Option **Anzeigen** steht nur zur Verfügung, wenn Sie als Format für Warnmeldungen **HTML** ausgewählt haben.

12 Aktivieren oder deaktivieren Sie **Fußzeilen für Warnung aktivieren**, um die Verwendung von Warnungsfußzeilen zu ermöglichen.

13 Geben Sie in das Texteingabefeld **Warnungsfußzeile** die Fußzeile für die Warnung ein.

14 Wählen Sie unter **Anzeigen** die Option **HTML-Inhalt (WYSIWYG)** oder **HTML-Inhalt (Quelle)** aus, je nachdem, ob der HTML-Text in der **Warnungsfußzeile** als kompilierter Code oder Quellcode angezeigt werden soll.

Die Option **Anzeigen** steht nur zur Verfügung, wenn Sie als Format für Warnmeldungen **HTML** ausgewählt haben.

15 Klicken Sie auf **Speichern** und dann auf **Übernehmen**.

Text für Haftungsausschluss

1 Wählen Sie unter **Richtlinien-Manager** die Option **Gateway**. Die Richtlinienseite für **Gateway** wird angezeigt.

2 Wählen Sie die gewünschte Richtlinie aus.

3 Klicken Sie auf **Text für Haftungsausschluss**. Die Registerkarte **Einstellungen anzeigen** für die Einstellungen des Texts für Haftungsausschluss wird angezeigt.

4 Aktivieren oder deaktivieren Sie unter **Aktivierung** das Kontrollkästchen **Aktivieren**, um die Einstellungen des Texts für Haftungsausschluss für die Richtlinie ein- oder auszuschalten.

5 Wählen Sie unter **Optionen** eine der folgenden Optionen aus:

- **Standardeinstellungen** — Ermöglicht die Anzeige und Konfiguration der Standardeinstellungen des Texts für Haftungsausschluss.
- Ein vorhandener Text für Haftungsausschluss.
- **neuen Optionssatz erstellen** — Ermöglicht das Erstellen eines neuen Optionssatzes der Einstellungen des Texts für Haftungsausschluss für eine ausgewählte Richtlinie.

Weitere Informationen hierzu finden Sie unter *Erstellen eines neuen Optionssatzes für Text für Haftungsausschluss auf Seite 171*.

- **Bearbeiten** — Ermöglicht die Änderung der Optionen von Einstellungen des Texts für Haftungsausschluss, die mit einer Richtlinie verknüpft sind.

Erstellen eines neuen Optionssatzes für Text für Haftungsausschluss

1 Wählen Sie unter **Richtlinien-Manager** die Option **Gateway**. Die Richtlinienseite für **Gateway** wird angezeigt.

2 Wählen Sie die gewünschte Richtlinie aus.

3 Klicken Sie auf **Text für Haftungsausschluss**. Die Registerkarte **Einstellungen anzeigen** für Text für Haftungsausschluss wird angezeigt.

4 Klicken Sie im Dropdown-Menü **Optionen** auf **neuen Optionssatz erstellen**. Die Seite **Text für Haftungsausschluss** wird angezeigt.

5 Geben Sie unter **Instanzname** einen Instanznamen für den Text für Haftungsausschluss an. Dieses Feld muss ausgefüllt werden.

6 Geben Sie unter **Haftungsausschlussnachricht (nur unformatierter Text)** den Text der Haftungsausschlussnachricht im Nur-Text-Format ein.

7 Wählen Sie im Dropdown-Menü **Haftungsausschluss einfügen** die Option **Vor dem Nachrichtentext**, **Hinter dem Nachrichtentext** oder **Als Anlage** aus, je nachdem, an welcher Stelle bzw. wie der Text für Haftungsausschluss in die E-Mail eingefügt werden soll.

8 Klicken Sie auf **Speichern** und dann auf **Übernehmen**.

Haftungsausschlüsse werden nur auf ausgehende E-Mails angewendet.

Gemeinsam benutzte Ressource

Zum Festlegen von Richtlinien kann es nützlich sein, wenn mehrere Richtlinien dieselben Ressourcen verwenden. Möglicherweise soll z. B. derselbe Text für Haftungsausschluss in zwei Richtlinien verwendet werden. Der Text für Haftungsausschluss kann als Ressource betrachtet werden, die von mehreren Richtlinien verwendet wird. Statt zwei Texten können Sie einen einzelnen Text für Haftungsausschluss erstellen, der von beiden Richtlinien genutzt werden kann.

Mit können Sie folgende Aktionen durchführen:

- Anzeigen von Einstellungen gemeinsam benutzter Ressourcen
- Erstellen neuer Ressourcen
- Ändern der Ressourceneinstellungen, sodass die Änderungen von allen Richtlinien übernommen werden, die die gemeinsam benutzten Ressourcen verwenden
- Löschen gemeinsam benutzter Ressourcen, die nicht mehr verwendet werden.

Einige Ressourcen können nicht gelöscht werden.

Die Seite enthält folgende drei Registerkarten:

- **Scanners und Warnungen**
- **Filterregeln**
- **Zeitintervalle**

Scanner und Warnungen

Unter **Scanner** können Sie die scannerbezogenen Einstellungen konfigurieren, die ein Richtlinie beim Scannen von Elementen verwendet. Sie haben folgende Möglichkeiten:

- **Kategorie** — Wählen Sie die Art der Einstellungen aus, die konfiguriert werden sollen. Folgende Optionen stehen zur Verfügung:
  - **Antivirenscanner**
  - **Anti-Spam**
  - **Anti-Phishing**
  - **Einstellungen für MIME-Nachrichten**
  - **Scannersteuerung**
  - **Warneinstellungen**
  - **Text für Haftungsausschluss**
  - **HTML-Dateien**
  - **Nachrichtengrößenfilterung**
- **Neue erstellen** — Erstellt eine neue gemeinsam benutzte Ressource für eine bestimmte Kategorie.

Weitere Informationen finden Sie unter *Erstellen einer neuen gemeinsam benutzten Ressource für „Antivirenscanner“*, *Erstellen einer neuen gemeinsam benutzten Ressource für „Anti-Spam“*, *Erstellen einer neuen gemeinsam benutzten Ressource für „Scannersteuerung“* und *Erstellen einer neuen gemeinsam benutzten Ressource für „Warneinstellungen“*

- **Löschen** — Ermöglicht das Löschen einer Ressource, die von keiner Richtlinie mehr verwendet wird. Einige Ressourcen können nicht gelöscht werden.
- **Bearbeiten** — Ermöglicht das Ändern der Ressourceneinstellungen.

Unter **Warnungen** stehen folgende Optionen zur Verfügung:

- **Kategorie** — Ermöglicht die Auswahl der zu konfigurierenden Warnmeldungstypen.
- **Neue erstellen** — Ermöglicht das Erstellen einer Warnmeldung. Der Text für Standardwarnungen wird angezeigt. Bearbeiten Sie diesen, um die neue Warnung zu erstellen.

Weitere Informationen hierzu finden Sie unter *Erstellen einer neuen Warnung auf Seite 133*.

- **Löschen** — Ermöglicht das Löschen einer Warnmeldung, die von keiner Richtlinie mehr verwendet wird.
- **Bearbeiten** — Ermöglicht das Ändern der Warnmeldung.
- **Umbenennen** — Ermöglicht das Umbenennen der Warnungskategorie.
- **Ansicht** — Ermöglicht das Anzeigen der Warnmeldung.

Sie können lediglich die Standardwarnungen für jede Art von Warnung anzeigen. Standardwarnungen können weder geändert noch gelöscht werden.

Erstellen einer neuen gemeinsam benutzten Ressource für „Antivirenscanner“

1. Klicken Sie unter **Richtlinien-Manager** auf **Gemeinsam benutzte Ressource**. Die Seite **Gemeinsam benutzte Ressourcen** wird geöffnet.
2. Wählen Sie auf der Registerkarte **Scanner und Warnungen** die Option **Antivirenscanner** im Dropdown-Menü **Kategorie** aus.
3. Klicken Sie im Bereich **Scanner** auf **Neue erstellen**. Die Seite **Einstellungen für Antivirenscanner** wird angezeigt.
4. Führen Sie die Schritte 5 bis 12 unter *Erstellen eines neuen Optionssatzes im Antivirenscanner auf Seite 127* aus.
5. Wählen Sie im Bereich **Warnungen** eine **Kategorie**.
6. Klicken Sie auf **Neue erstellen**, und führen Sie die Schritte unter *Erstellen einer neuen Warnung auf Seite 133* aus.

Erstellen einer neuen gemeinsam benutzten Ressource für „Anti-Spam“

1. Klicken Sie unter **Richtlinien-Manager** auf **Gemeinsam benutzte Ressource**. Die Seite **Gemeinsam benutzte Ressourcen** wird geöffnet.
2. Wählen Sie auf der Registerkarte **Scanner und Warnungen** die Option **Anti-Spam** im Dropdown-Menü **Kategorie** aus.
3. Klicken Sie im Bereich **Scanner** auf **Neue erstellen**. Die Seite **Anti-Spam-Einstellungen** wird angezeigt.
4. Führen Sie die Schritte 6 bis 16 unter *Erstellen eines neuen Optionssatzes für Anti-Spam-Einstellungen auf Seite 142* aus.
5. Wählen Sie im Bereich **Warnungen** eine **Kategorie**.
6. Klicken Sie auf **Neue erstellen**, und führen Sie die Schritte unter *Erstellen einer neuen Warnung auf Seite 133* aus.

Erstellen einer neuen gemeinsam benutzten Ressource für „Anti-Phishing“

1 Klicken Sie unter **Richtlinien-Manager** auf **Gemeinsam benutzte Ressource**. Die Seite **Gemeinsam benutzte Ressourcen** wird geöffnet.

2 Wählen Sie auf der Registerkarte **Scanner und Warnungen** die Option **Anti-Phishing** im Dropdown-Menü **Kategorie** aus.

3 Klicken Sie im Bereich **Scanner** auf **Neue erstellen**. Die Seite **Anti-Phishing-Einstellungen** wird angezeigt.

4 Führen Sie die Schritte 5 bis 7 unter *Erstellen eines neuen Optionssatzes für Anti-Phishing-Einstellungen auf Seite 147* aus.

5 Wählen Sie im Bereich **Warnungen** eine **Kategorie**.

6 Klicken Sie auf **Neue erstellen**, und führen Sie die Schritte unter *Erstellen einer neuen Warnung auf Seite 133* aus.

Erstellen einer neuen gemeinsam benutzten Ressource für „Einstellungen für MIME-Nachrichten“

1 Klicken Sie unter **Richtlinien-Manager** auf **Gemeinsam benutzte Ressource**. Die Seite **Gemeinsam benutzte Ressourcen** wird geöffnet.

2 Wählen Sie auf der Registerkarte **Scanner und Warnungen** die Option **Einstellungen für MIME-Nachrichten** im Dropdown-Menü **Kategorie** aus.

3 Klicken Sie im Bereich **Scanner** auf **Neue erstellen**. Die Seite **Nachrichteneinstellungen** wird mit vier Registerkarten angezeigt: **Optionen**, **Erweitert**, **MIME-Typen** und **Zeichensätze**.

4 Führen Sie die Schritte 5 bis 18 unter *Erstellen eines neuen Optionssatzes für MIME-Nachrichteneinstellungen auf Seite 161* aus.

5 Wählen Sie im Bereich **Warnungen** eine **Kategorie**.

6 Klicken Sie auf **Neue erstellen**, und führen Sie die Schritte unter *Erstellen einer neuen Warnung auf Seite 133* aus.

Erstellen einer neuen gemeinsam benutzten Ressource für „Scannersteuerung“

1 Klicken Sie unter **Richtlinien-Manager** auf **Gemeinsam benutzte Ressource**. Die Seite **Gemeinsam benutzte Ressourcen** wird geöffnet.

2 Wählen Sie auf der Registerkarte **Scanner und Warnungen** die Option **Scannersteuerung** im Dropdown-Menü **Kategorie** aus.

3 Klicken Sie im Bereich **Scanner** auf **Neue erstellen**. Die Seite **Scannersteuerung** wird angezeigt.

4 Geben Sie unter **Instanzname** einen Namen ein.

5 Geben Sie einen Wert unter **Maximale Verschachtelungsebene** ein.

6 Geben Sie einen Wert unter **Maximale dekomprimierte Dateigröße (MB)** ein.

7 Geben Sie einen Wert unter **Maximale Scandauer (Minuten)** ein.

8 Klicken Sie auf **Speichern**.

9 Wählen Sie im Bereich **Warnungen** eine **Kategorie**.

10 Klicken Sie auf **Neue erstellen**, und führen Sie die Schritte unter *Erstellen einer neuen Warnung auf Seite 133* aus.

Erstellen einer neuen gemeinsam benutzten Ressource für „Warneinstellungen“

1 Klicken Sie unter **Richtlinien-Manager** auf **Gemeinsam benutzte Ressource**. Die Seite **Gemeinsam benutzte Ressourcen** wird geöffnet.

2 Wählen Sie auf der Registerkarte **Scanner und Warnungen** die Option **Warneinstellungen** im Dropdown-Menü **Kategorie** aus.

3 Klicken Sie im Bereich **Scanner** auf **Neue erstellen**. Die Seite **Warneinstellungen** wird angezeigt.

4 Führen Sie die Schritte 5 bis 15 unter *Erstellen eines neuen Optionssatzes für Warneinstellungen auf Seite 170* aus.

5 Wählen Sie im Bereich **Warnungen** eine **Kategorie**.

6 Klicken Sie auf **Neue erstellen**, und führen Sie die Schritte unter *Erstellen einer neuen Warnung auf Seite 133* aus.

Erstellen einer neuen gemeinsam benutzten Ressource für „Text für Haftungsausschluss“

1 Klicken Sie unter **Richtlinien-Manager** auf **Gemeinsam benutzte Ressource**. Die Seite **Gemeinsam benutzte Ressourcen** wird geöffnet.

2 Wählen Sie auf der Registerkarte **Scanner und Warnungen** die Option **Text für Haftungsausschluss** im Dropdown-Menü **Kategorie** aus.

3 Klicken Sie im Bereich **Scanner** auf **Neue erstellen**. Die Seite **Text für Haftungsausschluss** wird angezeigt.

4 Führen Sie die Schritte 5 bis 8 unter *Erstellen eines neuen Optionssatzes für Text für Haftungsausschluss auf Seite 171* aus.

5 Wählen Sie im Bereich **Warnungen** eine **Kategorie**.

6 Klicken Sie auf **Neue erstellen**, und führen Sie die Schritte unter *Erstellen einer neuen Warnung auf Seite 133* aus.

Erstellen einer neuen gemeinsam benutzten Ressource für „HTML-Dateien“

1 Klicken Sie unter **Richtlinien-Manager** auf **Gemeinsam benutzte Ressource**. Die Seite **Gemeinsam benutzte Ressourcen** wird geöffnet.

2 Wählen Sie auf der Registerkarte **Scanner und Warnungen** die Option **HTML-Dateien** im Dropdown-Menü **Kategorie** aus.

3 Klicken Sie im Bereich **Scanner** auf **Neue erstellen**. Die Seite **HTML-Dateien** wird angezeigt.

4 Führen Sie die Schritte 5 bis 8 unter *Erstellen eines neuen Optionssatzes für HTML-Dateieinstellungen auf Seite 165* aus.

5 Wählen Sie im Bereich **Warnungen** eine **Kategorie**.

6 Klicken Sie auf **Neue erstellen**, und führen Sie die Schritte unter *Erstellen einer neuen Warnung auf Seite 133* aus.

Erstellen einer neuen gemeinsam benutzten Ressource für „ Nachrichtengrößenfilterung“

1 Klicken Sie unter **Richtlinien-Manager** auf **Gemeinsam benutzte Ressource**. Die Seite **Gemeinsam benutzte Ressourcen** wird geöffnet.

2 Wählen Sie auf der Registerkarte **Scanner und Warnungen** die Option **Nachrichtengrößenfilterung** im Dropdown-Menü **Kategorie** aus.

3 Klicken Sie im Bereich **Scanner** auf **Neue erstellen**. Die Seite **Nachrichtengrößenfilterung** wird angezeigt.

4 Führen Sie die Schritte 5 bis 8 unter *Erstellen eines neuen Optionssatzes für den Nachrichtengrößenfilter auf Seite 167* aus.

5 Wählen Sie im Bereich **Warnungen** eine **Kategorie**.

6 Klicken Sie auf **Neue erstellen**, und führen Sie die Schritte unter *Erstellen einer neuen Warnung auf Seite 133* aus.

Filterregeln

Unter **Regeln für Inhaltsscanner** können Sie die Regeln konfigurieren, die eine Richtlinie auf den Inhalt von E-Mails und Text in Anlagen anwenden kann. Sie haben folgende Möglichkeiten:

- **Kategorie** — Ermöglicht die Auswahl der zu konfigurierenden Regeltypen.
- **Neue Kategorie** — Ermöglicht das Erstellen einer neuen Regelkategorie.
- **Umbenennen** — Ermöglicht das Umbenennen einer Kategorie.

- **Löschen** — Ermöglicht das Löschen einer Kategorie, die nicht mehr benötigt wird.
- **Neue erstellen** — Ermöglicht das Erstellen einer neuen Regel.

Weitere Informationen hierzu finden Sie unter *Erstellen einer neuen Inhaltscannerregel auf Seite 179*.

- **Bearbeiten** — Ermöglicht das Ändern der Regeleinstellungen.
- **Löschen** — Ermöglicht das Löschen einer Regel, die von keiner Richtlinie mehr verwendet wird.

Der Link **Löschen** ist zweimal vorhanden. Der eine Link bezieht sich auf das Löschen einer Kategorie, die in der Dropdown-Liste enthalten ist, während der andere für das Löschen einer von Ihnen erstellten Regel bestimmt ist.

Jeder neuen Regel sollten Sie einen eindeutigen, aussagekräftigen Namen zuweisen. Vermeiden Sie aggressive oder provokante Namen, da sie in Benachrichtigungen enthalten sein können, die nach dem Auslösen einer Regel an Benutzer gesendet werden. Derartige Namen könnten außerdem dazu führen, dass die Benachrichtigungen gesperrt werden, da sie gesperrte Inhalte umfassen.

Unter **Dateifilterregeln** können Sie Regeln für Dateinamen, -typ und -größe festlegen. Sie haben folgende Möglichkeiten:

- **Neue erstellen** — Ermöglicht das Erstellen einer neuen Dateifilterregel.

Weitere Informationen hierzu finden Sie unter *Erstellen einer neuen Dateifilterregel auf Seite 180*.

- **Löschen** — Ermöglicht das Löschen einer Regel, die von keiner Richtlinie mehr verwendet wird.
- **Bearbeiten** — Ermöglicht das Ändern der Regeleinstellungen.

Beim Konfigurieren von Richtlinien können Sie die zu verwendenden Dateifilterregeln auswählen und die Reihenfolge festlegen, in der sie beim Scannen von Dateien angewendet werden.

Erstellen einer neuen Inhaltscannerregel

1 Klicken Sie unter **Richtlinien-Manager** auf **Gemeinsam benutzte Ressource**. Die Seite **Gemeinsam benutzte Ressourcen** wird geöffnet.

2 Klicken Sie auf die Registerkarte **Filterregeln**.

3 Klicken Sie im Bereich **Regeln für Inhaltsscanner** auf **Neue erstellen**. Die Seite **Neue Regel für Inhaltsscanner** wird angezeigt.

4 Geben Sie unter **Regelname** einen eindeutigen Namen ein.

5 Geben Sie unter **Details** im Feld **Beschreibung** eine Kurzbeschreibung der Regel ein.

6 Geben Sie auf der Registerkarte **Wort oder Ausdruck** unter **Die Regel wird ausgelöst, wenn das folgende Wort oder der folgende Ausdruck gefunden wird** die zu suchenden Wörter oder Ausdrücke ein.

7 Wählen Sie die gewünschten Optionen aus:

- **Groß-/Kleinschreibung ignorieren** — Wenn diese Option aktiviert ist, wird die Regel sowohl für groß- als auch für kleingeschriebene Wörter ausgelöst, die Sie angeben.
- **Beginn eines längeren Worts oder Ausdrucks** — Wenn diese Option aktiviert ist, wird die Regel für einen angegebenen Text ausgelöst, der mit dem Wort oder dem Ausdruck beginnt.
- **Platzhalter verwenden** — Wenn diese Option aktiviert ist, wird die Regel für das angegebene Wort oder den Ausdruck ausgelöst, das/der (ein) Platzhalterzeichen enthält. (Platzhalter werden häufig anstelle eines oder mehrerer Zeichen eingesetzt, wenn Sie beispielsweise das korrekte Zeichen nicht kennen oder nicht den gesamten Namen eingeben möchten.)
- **Ende eines längeren Worts oder Ausdrucks** — Wenn diese Option aktiviert ist, wird die Regel für einen angegebenen Text ausgelöst, der mit dem Wort oder dem Ausdruck endet.

8 Wählen Sie auf der Registerkarte **Dateiformat** die Option **Alles** aus, um alle Dateikategorien und deren Unterkategorien auszuwählen. Sie können innerhalb der ausgewählten Kategorien mehrere Kategorien und Dateitypen für die Übereinstimmung auswählen. Wenn Sie für die Unterkategorien **Alle** auswählen, werden dadurch alle bereits ausgewählten Optionen außer Kraft gesetzt.

9 Klicken Sie auf **Speichern** und dann auf **Übernehmen**.

Erstellen einer neuen Dateifilterregel

1 Klicken Sie unter **Richtlinien-Manager** auf **Gemeinsam benutzte Ressource**. Die Seite **Gemeinsam benutzte Ressourcen** wird geöffnet.

2 Klicken Sie auf die Registerkarte **Filterregeln**.

3 Klicken Sie im Bereich **Dateifilterregeln** auf **Neue erstellen**. Die Seite **Dateifilterregel** wird angezeigt.

4 Führen Sie die Anweisungen unter *Erstellen einer neuen Dateifilterregel auf Seite 138* aus.

Zeitintervalle

Unter **Zeitintervalle** können Sie verschiedene Zeitintervalle festlegen, die auf Richtlinien angewendet werden können. Sie haben folgende Möglichkeiten:

- **Ansicht** — Zeigt die Zeitintervalle unter **Immer** an.
- **Löschen** — Ermöglicht das Löschen eines Zeitintervalls, das von keiner Richtlinie verwendet wird.
- **Bearbeiten** — Ermöglicht das Ändern von Namen oder Zeiten für ein bestimmtes Zeitintervall.
- **Neue erstellen** — Ermöglicht das Erstellen eines neuen Zeitintervalls.

Erstellen eines neuen Zeitintervalls

1 Klicken Sie unter **Richtlinien-Manager** auf **Gemeinsam benutzte Ressource**. Die Seite **Gemeinsam benutzte Ressourcen** wird geöffnet.

2 Klicken Sie auf die Registerkarte **Zeitintervalle**.

3 Klicken Sie auf **Neue erstellen**. Die Seite **Zeitintervall** wird angezeigt.

4 Geben Sie unter **Namen des Zeitintervalls** einen eindeutigen Namen ein.

5 Wählen Sie unter **Tag und Uhrzeit auswählen** die gewünschten Tage aus.

6 Wählen Sie **Ganztägig** oder **Ausgewählte Stunden**, um die Stunden für das erstellte Zeitintervall anzugeben.
Wenn Sie **Ausgewählte Stunden** auswählen, wählen Sie in der Dropdown-Liste unter die Start- und Endzeiten aus.

7 Klicken Sie auf **Speichern** und dann auf **Übernehmen**.

Masterrichtlinien verwenden das Zeitintervall **Immer**. Wenn eine Richtlinie während eines anderen Zeitintervalls aktiv sein soll, müssen Sie eine Unterrichtlinie erstellen und ein anderes Zeitintervall angeben.

11 Einstellungen & Diagnose

In diesem Kapitel werden die Einstellungen und die Diagnose beschrieben, die Sie mit GroupShield für Exchange durchführen können.

Themen:

- *Einstellungen für Scan bei Zugriff*
- *Benachrichtigungen*
- *Anti-Spam*
- *Erkannte Elemente*
- *Voreinstellungen für Benutzeroberfläche*
- *Diagnose*
- *Produktprotokoll*
- *DAT-Einstellungen*
- *Import- und Exportkonfiguration*

Einstellungen für Scan bei Zugriff

Mit **Einstellungen für Scan bei Zugriff** werden die Einstellungen unter **Allgemein**, die Einstellungen für **Microsoft Virus Scanning API (VSAPI)** und die **Transport-Scan-Einstellungen** konfiguriert.

Für Exchange Server 2003

Standardmäßig ist der McAfee®-Transport-Scanner aktiviert und scannt alle E-Mails. Wenn Sie **Transport-Scan-Einstellungen** deaktivieren, scannt Microsoft® Virus Scanning API (VSAPI v 2.5) die E-Mails.

1 Klicken Sie auf **Einstellungen & Diagnose** | **Einstellungen für Scan bei Zugriff.** Die Seite **Einstellungen für Scan bei Zugriff** wird angezeigt.

2 Wählen Sie unter **Allgemein** die Option **Durchlassen** oder **Löschen**, je nachdem, welche Aktion bei Fehlschlagen des Scanvorgangs ausgeführt werden soll.

3 Gehen Sie unter **Microsoft Virus Scanning API (VSAPI)** folgendermaßen vor:

- Aktivieren oder deaktivieren Sie **Aktiviert**, um anzugeben, ob VSAPI aktiviert oder deaktiviert werden soll.

VSAPI wird auf sehr niedriger Ebene im Exchange-Informationsspeicher implementiert. Auf diese Weise kann eine Virenscananwendung mit hoher Leistung ausgeführt werden und wird gewährleistet, dass die Nachrichten gescannt werden, bevor ein Client auf sie oder zugehörige Anhänge zugreifen kann. Nachrichten und Anhänge brauchen daher nicht mehrmals gescannt werden (je nach Anzahl der Zielpostfächer), sondern werden vor ihrer Zustellung einmal gescannt. Durch das einmalige Scannen wird ebenfalls das erneute Scannen von Nachrichten verhindert, wenn diese kopiert werden, was zu einer Verbesserung der Systemleistung führt.

- Aktivieren oder deaktivieren Sie **Proaktives Scannen**, um anzugeben, ob E-Mails und Dateien beim Schreiben in den Speicher gescannt werden.

Das proaktive Scannen ist ein Scantyp, der von Microsoft® VSAPI ermöglicht wird. Über diesen Scan können Objekte aus dem Speicher nach ihrer Priorität gescannt werden.

Elemente, die in den Speicher gelangen und ihn verlassen, erhalten eine Prioritätsbewertung und werden in einer Scanwarteschlange abgelegt. Die Scanwarteschlange ermöglicht es, Elementen in der Warteschlange Prioritäten zuzuweisen und sie zu ändern.

Beispiel: Wenn ein Benutzer versucht, ein noch nicht gescanntes Element zu öffnen, erhält es eine höhere Priorität; Elemente, die in öffentlichen Ordnern gespeichert oder dorthin gesendet werden, erhalten hingegen eine niedrige Priorität. Dies wird als prioritätsbasierte Warteschlange bezeichnet.

Wenn alle Elemente hoher Priorität gescannt sind, beginnt der Scan von Elementen niedrigerer Priorität. Elemente, die zuerst eingingen, werden auch zuerst gescannt.

- Aktivieren oder deaktivieren Sie **Hintergrundscan**, um anzugeben, ob der Hintergrundscan aktiviert oder deaktiviert werden soll. Mit den Optionen **Aktivieren bei** und **Deaktivieren bei** können Sie den Hintergrundscan planen.

Der Hintergrundscan ist eine Art des Scannens bei Zugriff, was in Microsoft® Exchange 2003/2007 durch Microsoft® VSAPI ermöglicht wird. Hierbei werden nicht alle Dateien gescannt, wodurch die Scannerauslastung reduziert wird. Es werden die Datenbanken gescannt, für die das Scannen aktiviert wurde. Hintergrundscans sind standardmäßig deaktiviert.

- Geben Sie unter **Scan-Zeitsperre (Sekunden)** den Zeitraum ein, den auf einen Scanvorgang gewartet werden soll, bevor eine Zeitsperre eintritt.
- Aktivieren Sie die Option **Standard**, um die standardmäßige Anzahl der Scan-Threads zu verwenden, oder deaktivieren Sie die Option, und geben Sie den gewünschten Wert ein. Die Verwendung der Option **Standard** wird empfohlen.

4 Gehen Sie unter **Transport-Scan-Einstellungen** folgendermaßen vor:

- Wählen Sie **Aktiviert** aus, um die richtungsbasierte SMTP-Scansteuerung zu nutzen. Wird diese Option nicht ausgewählt, stehen die übrigen Optionen nicht zur Verfügung.
- Wählen Sie **Eingehende E-Mails scannen** aus, um Nachrichten von einem externen Server zu scannen (z. B. internetbasierte E-Mails). Wenn diese Option ausgewählt wird, die nächsten beiden Optionen aber nicht, werden an andere Domänen gesendete E-Mails nicht gescannt.
- Wählen Sie **Ausgehende E-Mails scannen**, um E-Mails zu scannen, die Ihre Exchange Server- oder Exchange-Organisation verlassen.
  Nachrichten werden als ausgehend angesehen, wenn mindestens ein Empfänger eine externe Adresse aufweist.
- Wählen Sie **Interne E-Mails scannen**, um E-Mails zu scannen, die von einem Ort innerhalb Ihrer Domäne an einen anderen Ort innerhalb Ihrer Domäne weitergeleitet werden.
  Nachrichten werden als intern angesehen, wenn Sie aus Ihrer Domäne stammen und ALLE Empfänger sich innerhalb Ihrer Domäne befinden.

Transport-Scans ermöglichen das Scannen von SMTP-Datenverkehr, bevor dieser in den Exchange-Informationsspeicher gelangt. Beim SMTP-Transport-Scan können weitergeleitete E-Mails, also E-Mails, die nicht für den lokalen Server bestimmt sind, gescannt werden, und ihre Zustellung kann verhindert werden. SMTP-Transport-Scans können auf Microsoft® Exchange 2003 mit VSAPI 2.5 angewendet werden.

5 Klicken Sie auf **Übernehmen**.

Für Exchange Server 2007

Die Hintergrundscan-Funktionen in GSE 7.0 wurden durch die neuen Funktionen aus VSAPI v 2.6 optimiert.

Ferner existiert für GroupShield für Exchange Server 2007 ein Stempelmechanismus. Nach dem Scannen einer E-Mail weist der McAfee®-Transport-Scanner der E-Mail-Kopfzeile einen Stempel zu. So wird das erneute Scannen der E-Mail durch Microsoft® Virus Scanning API (VSAPI) vermieden.

Die verbleibenden Funktionen entsprechen denen von Exchange Server 2003.

1. Klicken Sie auf **Einstellungen & Diagnose** | **Einstellungen für Scan bei Zugriff.** Die Seite **Einstellungen für Scan bei Zugriff** wird angezeigt.
2. Wählen Sie unter **Hintergrund-Scan-Einstellungen** die Option **Aktivieren** aus, oder heben Sie ihre Auswahl auf, um den Hintergrundscan zu aktivieren oder zu deaktivieren. Mit den Optionen **Aktivieren bei** und **Deaktivieren bei** können Sie den Hintergrundscan planen.
3. Wählen Sie **Nur Nachrichten mit Anlagen** aus, um den Hintergrundscan nur für E-Mails mit Anlagen zu aktivieren.
4. Wählen Sie **Nur nicht gescannte Objekte** aus, um den Hintergrundscan nur für noch nicht gescannte Nachrichten zu aktivieren.
5. Wählen Sie **Alles scannen erzwingen**, wenn Elemente unabhängig davon gescannt werden sollen, ob sie einen Scan-Zeitstempel aufweisen.
   Verfügt ein Element über einen Scan-Zeitstempel, bedeutet dies, dass das Element gescannt wurde und aktuell ist.
6. Wählen Sie **Scan-Zeitstempel aktualisieren** aus, um Hintergrundscans auf dem aktuellen Stand durchführen.
   Heben Sie die Auswahl dieser Option auf, wird der Stempel nicht aktualisiert. Diese Funktion ist hilfreich, wenn der Anbieter beispielsweise auf Nachrichten zugreifen, sie aber nicht unbedingt auf Viren scannen möchte.
7. Wählen Sie die Felder **Ab Datum** und **Bis Datum** aus, um die Aktualisierung des Scan-Zeitstempels zu planen.
   Es besteht ebenfalls die Möglichkeit, **Fristablauf** auszuwählen.
8. Gehen Sie unter **Transport-Scan-Einstellungen** folgendermaßen vor:
   - Wählen Sie **Aktivieren** aus, um den Transport-Scan zu aktivieren. Wird diese Option nicht ausgewählt, stehen die übrigen Optionen nicht zur Verfügung.
   - **Transport-Scan-Stempel** — Wählen Sie diese Option aus, um die richtigungsbasierte SMTP-Scansteuerung zu nutzen.

- **Eingehende E-Mails scannen** — Wählen Sie diese Option aus, um Nachrichten von einem externen Server zu scannen (z. B. internetbasierte E-Mails). Wenn diese Option ausgewählt wird, die nächsten beiden Optionen aber nicht, werden an andere Domänen gesendete E-Mails nicht gescannt.
- **Ausgehende E-Mails scannen** — Wählen Sie diese Option aus, um E-Mails zu scannen, die Ihre Exchange Server- oder Exchange-Organisation verlassen. Nachrichten werden als ausgehend angesehen, wenn mindestens ein Empfänger eine externe Adresse aufweist.
- **Interne E-Mails scannen** — Wählen Sie diese Option aus, um E-Mails zu scannen, die von einem Ort innerhalb Ihrer Domäne an einen anderen Ort innerhalb Ihrer Domäne weitergeleitet werden.
  Nachrichten werden als intern angesehen, wenn Sie aus Ihrer Domäne stammen und ALLE Empfänger sich innerhalb Ihrer Domäne befinden.

Geben Sie unter **Microsoft Virus Scanning API (VSAPI)** im Feld **Unteres Alterslimit (Sekunden)** einen Wert ein, um anzugeben, ob alle E-Mails gescannt werden sollen oder nur diejenigen, deren Datum und Uhrzeit vor den Angaben in der Einstellung liegen. Dies ist nützlich, wenn der Kunde beispielsweise einen Befall bzw. eine Infektion der E-Mails vermutet, die innerhalb der letzten 2 Tage eingegangen sind.
Der Hintergrundscan wird dadurch ferner schneller beendet und die Auslastung des Servers reduziert.

9 Klicken Sie auf **Übernehmen**.

Benachrichtigungen

Mithilfe von Benachrichtigungseinstellungen kann der Benutzer Inhalt und SMTP-Adresse zum Senden von E-Mail-Benachrichtigungen für den Administrator konfigurieren.

1 Klicken Sie auf **Einstellungen & Diagnose** | **Benachrichtigungen**. Die Seite **Benachrichtigungen** wird angezeigt.

2 Geben Sie unter **E-Mail-Adresse des Administrators** die E-Mail-Adresse des Administrators ein, um Benachrichtigungen an das Administrator-E-Mail-Konto des betreffenden Exchange-Servers zu senden.

3 Geben Sie unter **E-Mail-Adresse des Absenders** die E-Mail-Adresse des Absenders ein, um Benachrichtigungen unter Verwendung der Absenderadresse zu senden.

4 Geben Sie unter **Betreffzeile für Benachrichtigung** eine Betreffzeile ein, um Benachrichtigungen unter Verwendung des Betreffzeileninhalts zu senden.

5 Klicken Sie unter **Benachrichtigungstext** auf **Bearbeiten**, um den Benachrichtigungstext zu ändern, der in der Nachricht enthalten sein soll.

Sie können weitere *Benachrichtigungsfelder* verwenden, um eine benutzerdefinierte Benachrichtigung zu erstellen.

6 Wählen Sie **Task 'Ergebnisbenachrichtigung' aktivieren** aus, um E-Mails mit den Ergebnissen von Scans bei Zugriff und Aktualisierungstasks zu senden. Die E-Mail wird im HTML-Format gesendet. Ihre Daten und ihr Format entsprechen dem Fenster **Taskergebnisse** in der Benutzeroberfläche. Diese Funktion kann über diese Option aktiviert oder deaktiviert werden. Standardmäßig ist diese Funktion deaktiviert.

7 Klicken Sie auf **Übernehmen**.

Folgende Benachrichtigungsfelder stehen zur Verfügung:

- %dts% — Datum und Zeit
- %sdr% — Absender
- %ftr% — Filter
- %fln% — Dateiname
- %rul% — Regelname
- %act% — Ausgeführte Aktion
- %fdr% — Ordner
- %vrs% — Erkennungsname
- %trs% — Status (Trainingsstatus)
- %tik% — Ticketnummer
- %idy% — Gescannt durch
- %psn% — Richtlinienname
- %svr% — Server
- %avd% — AV DAT
- %ave% — AV Engine (AV-Modul)
- %rpt% — Empfänger
- %rsn% — Grund
- %sbj% — Betreff

- %ssc% — Spamfaktor
- %ase% — Anti-Spam-Modul
- %asr% — Anti-Spam-Regeln

Anti-Spam

Mit den **Anti-Spam-Einstellungen** können Sie **Gateway-Spam-Filter** und **Weiterleitung Benutzermüllordner** konfigurieren.

1. Klicken Sie auf **Einstellungen & Diagnose** | **Anti-Spam**. Die Seite **Anti-Spam-Einstellungen** wird angezeigt.
2. Geben Sie eine E-Mail-Adresse ein, um die **Adresse des Systemmüllordners** zum Filtern von Müllmails zu konfigurieren.
3. Wählen Sie **Weiterleitung an Benutzermüllordner auf diesem Server aktivieren** aus, um Müllmails an den Benutzermüllordner auf dem Mailserver weiterzuleiten.
4. Klicken Sie auf **Übernehmen**.

Erkannte Elemente

Unter **Erkannte Elemente** haben Sie die folgenden Möglichkeiten:

- Geben Sie an, ob die lokale Datenbank oder der McAfee Quarantine Manager zum Isolieren von E-Mails verwendet werden soll.
- Konfigurieren Sie die Einstellungen für die Kommunikation mit dem McAfee Quarantine Manager.
- Konfigurieren Sie die Wartungseinstellungen für die lokale Quarantäne-Datenbank.

McAfee Quarantine Manager

1. Klicken Sie auf **Einstellungen & Diagnose** | **Erkannte Elemente**. Die Seite **Erkannte Elemente** wird angezeigt.
2. Wählen Sie **Aktiviert** aus, um den McAfee Quarantine Manager als Repository zum Isolieren erkannter Elemente zu verwenden.
   Wird diese Option nicht ausgewählt, stehen die übrigen Optionen nicht zur Verfügung.

3 Geben Sie unter **IP-Adresse** die IP-Adresse des Servers ein, auf dem der McAfee Quarantine Manager ausgeführt wird.

4 Geben Sie unter **Port** die Portnummer für den McAfee Quarantine Manager an, die GroupShield für Exchange zum Senden von Informationen zur Spam-Erkennung sowie anderen Informationen an den McAfee Quarantine Manager verwenden soll. Die Standardportnummer ist 49500.

5 Geben Sie unter **Rückrufport** die GroupShield für Exchange-Portnummer an, die McAfee Quarantine Manager für die Freigabe von E-Mails oder zum Senden von Konfigurationsinformationen an GroupShield für Exchange verwendet.

6 Klicken Sie auf **Übernehmen**.

Weitere Informationen zur Verwendung des McAfee Quarantine Managers finden Sie im *Produkthandbuch von McAfee Quarantine Manager v 4.1*.

Lokale Datenbank

1 Wählen Sie unter **Pfad der Datenbank angeben** im ersten Feld (in der Dropdown-Liste) die Art des **Datenbankpfads** aus, und geben Sie im zweiten Feld einen entsprechenden Pfad an.

2 Geben Sie unter **Maximale Elementgröße (MB)** die maximale Größe eines in der Datenbank zu speichernden Elements ein.

3 Geben Sie unter **Maximale Abfragegröße (Datensätze)** die maximale Anzahl an Datensätzen ein, die zurückgegeben werden können, wenn die lokale Quarantäne-Datenbank eine Abfrage empfängt.

4 Geben Sie unter **Maximales Elementalter (Tage)** die maximale Anzahl an Tagen ein, die ein Element in der lokalen Quarantäne-Datenbank verbleibt, bis es für den Löschvorgang vorgesehen wird.

5 Klicken Sie auf **Zeitplan bearbeiten** der Option **Häufigkeit für Bereinigung alter Elemente**, um anzugeben, wie oft alte, für den Löschvorgang vorgesehene Elemente aus der Datenbank gelöscht werden sollen.

6 Klicken Sie auf **Zeitplan bearbeiten** der Option **Optimierungshäufigkeit**, um anzugeben, wie oft die Datenbank optimiert wird.

7 Klicken Sie auf **Übernehmen**.

Voreinstellungen für Benutzeroberfläche

Unter **Voreinstellungen für Benutzeroberfläche** können Sie die Aktualisierungshäufigkeit für die Benutzeroberfläche sowie Einstellungen für Berichte, Metrik, Grafiken und Diagramme festlegen.

Dashboardeinstellungen

1. Klicken Sie auf **Einstellungen & Diagnose** | **Voreinstellungen für Benutzeroberfläche**. Die Seite **Voreinstellungen für Benutzeroberfläche** wird angezeigt.
2. Wählen Sie auf der Registerkarte **Dashboardeinstellungen** die Option **Automatische Aktualisierung**, um anzugeben, ob die im Dashboard angezeigten Informationen automatisch aktualisiert werden sollen.
3. Geben Sie unter **Aktualisierungsrate (Sekunden)** die Dauer in Sekunden ein, damit die Informationen im Dashboard nach Ablauf dieses Zeitraums aktualisiert werden.
4. Wählen Sie **Berichte aktivieren** aus, um die Berichtserstellung zu aktivieren oder zu deaktivieren.
5. Wählen Sie **Vor kurzem gescannte Elemente anzeigen** aus, um festzulegen, ob die vor kurzem gescannten Elemente in den Berichten berücksichtigt werden sollen.
6. Legen Sie unter **Maximale Anzahl vor kurzem gescannter Elemente** die maximale Anzahl an vor kurzem gescannten Elementen fest, die in den Berichten berücksichtigt werden sollen.
7. Geben Sie unter **Diagrammmaßstab (Einheiten)** die Maßeinheiten für den Maßstab des zu erzeugenden Diagramms ein.
8. Geben Sie unter **Anzahl Stunden für Bericht** das Intervall (in Stunden) für die Erstellung von Berichten ein.
9. Klicken Sie auf **Übernehmen**.

Einstellungen für Grafiken und Diagramme

1. Wählen Sie auf der Registerkarte **Einstellungen für Grafiken und Diagramme** die Option **3D** aus, um anzugeben, ob das Dashboarddigramm in dreidimensionaler (3D) Form angezeigt werden soll.
2. Wählen Sie **Transparent zeichnen** aus, um festzulegen, ob die Balken in einem dreidimensionalen Balkendiagramm gefüllt oder transparent angezeigt werden sollen. Durch gefüllte Balken werden alle dahinter liegenden Balken verdeckt. Bei transparenten Balken bleibt der Blick auf dahinter liegende transparente Balken frei.

3 Wählen Sie **Anti-Aliasing** aus, um festzulegen, ob bei der Anzeige von Kreisdiagrammen Anti-Aliasing-Techniken verwendet werden sollen. Wenn Sie Anti-Aliasing verwenden, sind die Kurven von Kreisdiagrammen glatter. Ohne Anti-Aliasing erscheinen die Kurven in Kreisdiagrammen gezackt.

4 Wählen Sie **Explodierter Kreis** aus, um festzulegen, ob die Kreissegmente des Kreisdiagramms wirklich als Kreis oder mit einigem Abstand zwischen den einzelnen Segmenten angezeigt werden sollen.

5 Legen Sie unter **Kreiswinkel (Grad)** den beim Erstellen von Kreisdiagrammen zu verwendenden Winkel fest.

6 Klicken Sie auf **Übernehmen**.

Diagnose

Geben Sie unter **Diagnose** die erforderliche Ebene für die Fehlersuchprotokollierung, die maximal zulässige Größe der Fehlersuchprotokolldateien und den Speicherort für diese Dateien an. Sie können die Einstellungen für den Fehlerberichterstellungsdienst konfigurieren und die Ereignisse bestimmen, die im Produkt- und Ereignisprotokoll aufgezeichnet werden sollen, indem Sie den Speicherort des Produktprotokolls, den Namen, Größenbeschränkungen und Zeitüberschreitungseinstellungen festlegen.

Fehlersuchprotokollierung

1 Klicken Sie auf **Einstellungen & Diagnose** | **Diagnose**. Die Seite **Diagnose** wird angezeigt.

2 Geben Sie auf der Registerkarte **Fehlersuchprotokollierung** im Dropdown-Menü **Ebene** die Art der Informationen an, die im Fehlersuchprotokoll erfasst werden sollen. Sie haben folgende Möglichkeiten:

- **Hoch** — Erfasst eine große Anzahl von Protokolleinträgen.
- **Mittel** — Erfasst eine mittlere Anzahl von Protokolleinträgen.
- **Niedrig** — Erfasst eine geringe Anzahl von Protokolleinträgen.
- **Ohne** — Deaktiviert die Fehlersuchprotokollierung.

3 Wählen Sie **Größenlimit für Fehlersuchprotokolldateien** aus, um eine Größenbeschränkung für Fehlersuchprotokolldateien festzulegen. Geben Sie unter **Maximale Größe der Fehlersuchprotokolldatei** die maximale Größe (in Megabyte oder Kilobyte) der Fehlersuchprotokolldateien ein.

4 Wählen Sie **Pfad für Fehlersuchdateien angeben** aus, um einen Pfad für Fehlersuchdateien festzulegen. Nehmen Sie eine Auswahl in der Dropdown-Liste vor, und geben Sie den entsprechenden Pfad an:

- **(Vollständiger Pfad)**
- **<Desktop>**
- **<Installationsordner>**
- **<Systemlaufwerk>**
- **<Programmdateien>**
- **<Windows-Ordner>**

Setzen Sie die Fehlersuchprotokollierung sorgfältig ein, da sie viel Speicherplatz auf der Festplatte belegt und die gesamte Leistung des Exchange-Servers beeinträchtigt. Sie sollte nur für einen begrenzten Zeitraum aktiviert werden, der von einem autorisierten Mitarbeiter (McAfee-Supportechniker) empfohlen wurde.

Fehlerberichterstellungsdienst

1 Wählen Sie auf der Registerkarte **Fehlerberichterstellungsdienst** die Option **Aktivieren** aus, um den Fehlerberichterstellungsdienst zu aktivieren oder zu deaktivieren.

2 Wählen Sie **Ausnahmen abfangen** aus, um Informationen über Ausnahmeereignisse, wie z. B. Systemabstürze, zu erfassen.

3 Wählen Sie **Ausnahmen an Benutzer melden** aus, um anzugeben, ob Ausnahmen dem Administrator gemeldet werden sollen.

Ereignisprotokollierung

1 Wählen Sie auf der Registerkarte **Ereignisprotokollierung** unter **Produktprotokoll** die Option **Ereignisse vom Typ 'Information' schreiben**, **Ereignisse vom Typ 'Information' schreiben** und **Ereignisse vom Typ 'Fehler' schreiben**, um die jeweiligen Ereignisse in das Produktprotokoll aufzunehmen.

2 Wählen Sie unter **Ereignisprotokoll** die Option **Ereignisse vom Typ 'Information' schreiben**, **Ereignisse vom Typ 'Information' schreiben** und **Ereignisse vom Typ 'Fehler' schreiben**, um die jeweiligen Ereignisse in das Ereignisprotokoll aufzunehmen.

Produktprotokoll

Auf der Registerkarte **Produktprotokoll** können Sie den Pfad, die Größenbeschränkung und die Einstellungen für das Abfragezeitlimit eines Produktprotokolls festlegen.

1 Aktivieren Sie im Abschnitt **Pfad** die Option **Pfad der Datenbank angeben**, um festzulegen, ob der Standardpfad oder ein anderer Pfad für das Produktprotokoll verwendet werden soll.
Bei Deaktivierung wird der Standardpfad verwendet. Bei aktivierter Option nehmen Sie eine Auswahl in der Dropdown-Liste vor, und geben Sie den entsprechenden Pfad an:

- **(Vollständiger Pfad)**
- **<Desktop>**
- **<Installationsordner>**
- **<Systemlaufwerk>**
- **<Programmdateien>**
- **<Windows-Ordner>**

2 Aktivieren Sie **Dateiname der Datenbank angeben**, um festzulegen, ob der Standardname oder ein anderer Name verwendet werden soll. Wenn die Option deaktiviert ist, wird der Standarddateiname verwendet. Der standardmäßige **Datenbank-Dateiname** lautet **productlog.bin**.

3 Gehen Sie im Abschnitt **Größenlimits** folgendermaßen vor:

- Wählen Sie **Datenbankgröße begrenzen** aus, um die Größe der Produktprotokolldatenbank zu begrenzen.
- Geben Sie unter **Maximale Datenbankgröße** einen Wert für die Produktprotokolldatenbank ein. Die Größe kann entweder in Megabyte oder in Kilobyte angegeben werden.
- Wählen Sie **Alterslimit für Einträge** aus, um einen festgelegten Zeitraum anzugeben, nach dem die Produktprotokolleinträge gelöscht werden sollen.
- Geben Sie unter **Maximales Eintragsalter** einen Wert ein, um die Anzahl der Tage festzulegen, die ein Eintrag bis zum Löschen in der Datenbank verbleiben soll.

4 Gehen Sie im Abschnitt **Erweitert** folgendermaßen vor:

- Wählen Sie **Abfragezeitlimit angeben** aus, um die zulässige Zeitdauer für die Beantwortung einer Produktprotokollabfrage festzulegen.
- Geben Sie unter **Abfragezeitlimit (Sekunden)** einen Wert ein, um die maximal zulässige Anzahl an Sekunden für die Beantwortung einer Produktprotokollabfrage festzulegen.

5 Klicken Sie auf **Übernehmen**.

Produktprotokoll

Sie können **Produktprotokoll** verwenden, um Suchfilter einzurichten, die Sie beim Auffinden von Informationen im Produktprotokoll unterstützen. Weiterhin können die Ergebnisse der Suche angezeigt werden.

So suchen Sie nach Erkennungen

1 Klicken Sie auf **Einstellungen & Diagnose** | **Produktprotokoll**. Die Seite **Produktprotokoll** wird geöffnet.

2 Wählen Sie im Abschnitt **Produktprotokoll** mindestens einen der folgenden Filter aus:

- **ID** — Geben Sie die Nummer eines bestimmten Produktprotokolleintrags ein.
- **Ebene** — Wählen Sie je nach anzuzeigendem Protokolltyp in der Dropdown-Liste im zweiten Feld **Informationen**, **Warnung** oder **Fehler** aus.
- **Beschreibung** — Wählen Sie die entsprechende Beschreibung aus.

Sie können bis zu drei Suchfilter auswählen.

3 Wählen Sie das Optionsfeld **Alle Datumsangaben** aus, um alle Einträge zu berücksichtigen, oder **Datumsbereich**, und geben Sie den gewünschten Datumsbereich im Dropdown-Menü an.

4 Klicken Sie auf **Suchen**. Im Abschnitt **Ergebnisse anzeigen** wird eine Liste der erkannten Elemente angezeigt, die Ihren Suchkriterien entsprechen.

Klicken Sie auf **Filter löschen**, um die Standardeinstellungen für Suchfilter wiederherzustellen, und auf **In CSV-Datei exportieren**, um die Liste der Erkennungen im CSV-Format zu exportieren.

5 Klicken Sie auf **Übernehmen**.

DAT-Einstellungen

Bei DAT-Dateien handelt es sich um die Definitionsdateien für die Erkennung. Diese Dateien werden auch als Signaturdateien bezeichnet und enthalten die Code-Signaturen die erforderlich sind, damit Virenschutz- und/oder Anti-Spyware-Programme Viren, Trojanische Pferde und potenziell unerwünschte Programme erkennen und entfernen können.

1 Klicken Sie auf **Einstellungen & Diagnose** | **DAT-Einstellungen**. Die Seite **DAT-Einstellungen** wird angezeigt.

2 Geben Sie unter **Maximale Anzahl alter DATs** die maximale Anzahl der DAT-Generierungen ein, die während der regelmäßigen Aktualisierungen im System gespeichert werden sollen. Der Standardwert ist 10.

3 Klicken Sie auf **Übernehmen**.

Konfiguration importieren und exportieren

Unter **Konfigurationen importieren und exportieren** haben Sie folgende Möglichkeiten:

- Kopieren der Konfiguration des Exchange-Servers in einen Bereich, aus dem sie von einem anderen Exchange-Server importiert werden kann.
- Anwenden der Konfiguration eines anderen Exchange-Systems auf dieses System.
- Festlegen des Pfades, aus dem automatische Aktualisieren heruntergeladen werden. Pfadinformationen werden in einer Standortliste gespeichert. Die gewünschte Standortliste kann festgelegt werden.

Die Registerkarten **Konfiguration** und **Standortliste** stehen zur Verfügung.

Konfiguration

Sie können die Konfiguration dieses Exchange Server-Systems kopieren und in einem Pfad ablegen, aus dem es von anderen Exchange Server-Systemen importiert werden kann. Gehen Sie dazu folgendermaßen vor:

1 Klicken Sie auf **Einstellungen & Diagnose** | **Import- und Exportkonfiguration**. Die Seite **Import- and Exporteinstellungen** wird geöffnet.

2 Wählen Sie die Registerkarte **Konfiguration** aus.

3 Klicken Sie auf **Exportieren**.

4 Geben Sie den Pfad zum Speichern der Datei an.

5 Klicken Sie auf **Speichern** und dann auf **Übernehmen**.

Importieren einer anderen Konfiguration für dieses Exchange Server-System:

1 Klicken Sie auf **Einstellungen & Diagnose** | **Import- und Exportkonfiguration**. Die Seite **Import- and Exporteinstellungen** wird geöffnet.

2 Wählen Sie die Registerkarte **Konfiguration** aus.

3 Verwenden Sie das Feld **Dateiname** oder die Schaltfläche **Durchsuchen**, um nach der zu importierenden Konfigurationsdatei zu suchen.

4 Klicken Sie auf **Importieren**, um diese Konfiguration zu importieren.

Klicken Sie auf **Standard wiederherstellen**, um die Standardeinstellungen und -werte aus der Datei **McAfeeConfig.xml** wiederherzustellen.

Standortliste

Mit einer Standortliste wird angegeben, von wo automatische Aktualisierungen heruntergeladen werden.

Standardmäßig verwendet GroupShield eine Standortliste, die für automatische Aktualisierungen auf eine McAfee-Site verweist. Sie können jedoch auch eine Standortliste verwenden, die auf einen anderen Speicherort verweist.

Wenn Sie bereits eine alternative Standortliste erstellt haben, die Sie importieren möchten:

1 Verwenden Sie auf der Registerkarte **Standortliste** das Feld **Dateiname** oder **Durchsuchen**, um zu der gewünschten Datei **Sitelist.xml** zu wechseln.

Die Datei **Sitelist.xml** erhalten Sie, indem eine Repository-Liste vom ePolicy Orchestrator-Server oder McAfee AutoUpdate Architect-Server exportiert wird.

2 Klicken Sie auf **Importieren**. Die neue Standortliste ersetzt die vorhandene Standortliste bzw. die Standardstandortliste.

3 Klicken Sie auf **Übernehmen**.

Stichwortverzeichnis

A

Aktualisieren von GroupShield 38
Alle Elemente 113
Alle Scanner auflisten 120
Ändern eines vorhandenen Scans auf Anforderung 101
Ändern von GroupShield 46
Anti-Phishing 146
Anti-Spam-Einstellungen 187
Antivirenscanner 125
  Aktionen 131
  Bearbeiten von Aktionen 130
  neuen Optionssatz erstellen 127
Auslöseregeln 119
Avert Labs-Bedrohungsbibliothek 19
Avert Labs-Virenschutz-Center 19

B

Bedrohungsbibliothek 19
Benachrichtigungseinstellungen 185
Benutzer angeben 123
Berichte 99
Beschädigter Inhalt 148
Beta-Programmwebsite 19

D

Dashboard 96
DAT-Dateien
  Aktualisierungen, Website 19
  Avert Labs-Benachrichtigungsdienst für Aktualisierungen 19
Dateifilterung 137
DAT-Einstellungen 194
Diagnose 190
  Ereignisprotokollierung 191
  Fehlerberichterstellungsdienst 191
  Fehlersuchprotokollierung 190
  Produktprotokoll 191
Download-Site 19

E

EICAR 41
Einfache Berichte 105
Einführung in ProtectionPilot 84
Einstellungen anzeigen 123
Einstellungen der lokalen Datenbank 188
Einstellungen für den McAfee Quarantine Manager 187
Einstellungen für erkannte Elemente 187
Einstellungen für MIME-Nachrichten 159
Einstellungen für Scan bei Zugriff 182
Entfernen von GroupShield 48
ePolicy Orchestrator
  Deinstallation 65
  Installation 52
  Voraussetzungen 50
ePolicy Orchestrator-Berichte 63
ePolicy Orchestrator-Konsole 50
Erstellen einer neuen Warnung 133
Erstellen einer Unterrichtlinie 119
Erweiterte Berichte 105
Evaluieren von McAfee-Produkten, Download-Site 19

F

Filterregeln 177

G

Gemeinsam benutzte Ressource 172
Geschützter Inhalt 150
Gesperrte Dateitypen/ Nachrichten 113
GroupShield 8

H

Hintergrundinstallation 32
Hinzufügen einer neuen Inhaltsregel 135
Hinzufügen von Scannern/ Filtern 122
HotFix- und Patch-Veröffentlichungen (für Produkte und Sicherheitsschwachstellen) 19
HTML-Dateien 164

I

Import- und Exporteinstellungen 194
  Konfiguration 194
  Standortliste 195
Inhaltsscan 132
Inhaltsscan-Aktionen 136
Installieren von Anti-Spam für Exchange 32
Installieren von GroupShield 26
Installieren zusätzlicher Komponenten 30

J

Jetzt ausführen 102, 104

K

Kennwortgeschützte Dateien 154
KnowledgeBase-Suche 19
Konfigurieren von GroupShield - Clusterumgebung 34
Konfigurieren von GroupShield-Richtlinien 57
Kontaktinformationen 19
Konventionen in diesem Handbuch 17
Kundendienst, Kontakt 19

L

Löschen eines Scans auf Anforderung 102

M

Masterrichtlinie 120
McAfee Quarantine Manager (MQM) 43
Muster übermitteln, Avert Labs WebImmune 19

N

Nachrichtengrößenfilterung 166
Neue Dateifilterregel 138
Neue Funktionen von GroupShield 12

P

Phishing 109
Planen eines neuen Scans auf Anforderung 100
Planen von Tasks in ePolicy Orchestrator 59
Produktinformationen, Finden 18
Produktprotokoll 193
Produkt-Upgrades 19
Professional Services, McAfee-Ressourcen 19
ProtectionPilot
- Deinstallation 86
- Einrichten und Durchsetzen von Richtlinien 87
- Installation 85
- Planen von Tasks 90
- Voraussetzungen 83

PUP 111

R

Ressourcen, für Produktinformationen 18
Richtlinien-Manager 117
- Erweiterte Ansicht 118
- Vererbungsansicht 118

Richtlinientypen 124

S

Scannersteuerung 156
Scans auf Anforderung 99
- Ändern 101
- Löschen 102
- Planen 100

Schulung, McAfee-Ressourcen 19
Schutz vor Pufferüberläufen 31, 98
ServicePortal, technischer Support 19
Sicherheitsaktualisierungen, DAT-Dateien und Modul 19
Sicherheitsschwachstellen, Veröffentlichungen 19
Sicherheitszentrale (*siehe* Avert Labs)
Signierter Inhalt 152
Single Copy Cluster 35
Spam 108
Statistik & Informationen 97
Statistiken 97
Statusbericht
- Ändern 104
- Löschen 104
- Planen 103

T

Technischer Support, Kontakt 19
Testen der GroupShield-Installation 41
Text für Haftungsausschluss 171
Transport-Scan 183

U

Unerwünschter Inhalt 112
Unterrichtlinie erstellen 119
Upgrade-Website 19

V

Verschiedene Einstellungen 169
Verschlüsselter Inhalt 152
Versionen und Aktualisierungen 98
Virenschutz-Center (*siehe* Avert Labs)
Virtual Technician 43
Virus 110
Virusinformationsbibliothek (*siehe* Avert Labs-Bedrohungsbibliothek)
Voreinstellungen für Benutzeroberfläche 189
- Dashboardeinstellungen 189
- Einstellungen für Grafiken und Diagramme 189

VSAPI 182

W

Warneinstellungen 169
WebImmune, Avert Labs-Virenschutz-Center 19

Z

Zeitintervalle 180
Zielgruppe 17
Zuweisen einer Inhaltsregel 133

700-1705-15

Copyright © 2007 McAfee, Inc. Alle Rechte vorbehalten.

McAfee®

mcafee.com